NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DECREASING VARIANCE IN RESPONSE TIME TO SINGULAR INCIDENTS OF PIRACY IN THE HORN OF AFRICA AREA OF OPERATION

by

Ryan O'Connell
and
Christopher Descovich

June 2010

Thesis Advisor: Steven J. Iatrou
Second Reader: Daniel F. Warren

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Decreasing Variance in Response Time to Singular Incidents of Piracy in the Horn of Africa Area of Operation			**5. FUNDING NUMBERS**
6. AUTHOR(S) Ryan O'Connell, Christopher Descovich			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol Number:_______________.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**
13. ABSTRACT (maximum 200 words) Instances of piracy have been increasing since 2006 and the international community can ignore this problem no more. Legal, socio-economic, and technological issues hinder multi-national efforts to combat piracy effectively. Response to events of piracy are oftentimes late, as reporting of incidents is also mired in legal issues; however, technology does exist that can notify companies that a ship is being attacked by pirates as the attack occurs or possibly prior to the attack if the attackers display intent. This technology is the Ship Security Alert System (SSAS) and The International Maritime Organization (IMO) has mandated that all ships greater than 500 gross tons (United States Coast Guard, 2004) shall be equipped with an SSAS. The problem lies in who should receive the SSAS attack alert notification. Currently, these distress signals only go to the company that owns the ship. This thesis will investigate the implications of SSAS reports directly fed to existing Navy networks and show that small changes to existing Navy Maritime Operations C2 structure could result in an optimization in force employment and timeliness of response.			
14. SUBJECT TERMS Piracy, MOC, SSAS, POW-ER, HOA, Somalia, Merchant shipping			**15. NUMBER OF PAGES** 111
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DECREASING VARIANCE IN RESPONSE TIME TO SINGULAR INCIDENTS OF PIRACY IN THE HORN OF AFRICA AREA OF OPERATION

Ryan J. O'Connell
Lieutenant, United States Navy
B.S., United States Naval Academy, 2002

Christopher M. Descovich
Lieutenant, United States Navy
B.S., California Maritime Academy, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
June 2010

Authors: Ryan O'Connell

Chris Descovich

Approved by: Steven J. Iatrou
Thesis Advisor

Daniel F. Warren
Co-Advisor

Daniel C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Instances of piracy have been increasing since 2006, and the international community can ignore this problem no more. Legal, socio-economic, and technological issues hinder multi-national efforts to combat piracy effectively. Response to events of piracy are oftentimes late, as reporting of incidents is also mired in legal issues; however, technology does exist that can notify companies that a ship is being attacked by pirates as the attack occurs or possibly prior to the attack if the attackers display intent. This technology is the Ship Security Alert System (SSAS), and The International Maritime Organization (IMO) has mandated that all ships greater than 500 gross tons (United States Coast Guard, 2004) shall be equipped with an SSAS. The problem lies in who should receive the SSAS attack alert notification. Currently, these distress signals only go to the company that owns the ship. This thesis will investigate the implications of SSAS reports directly fed to existing Navy networks, and show that small changes to existing Navy Maritime Operations C2 structure could result in an optimization in force employment and timeliness of response.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AB	Able Bodied Seaman
AOR	Area of Operation
C2	Command and Control
CCIR	Commander’s Critical Information Requirements
CCRP	Command and Control Research Program
CE	Chief Engineer
CINCPAC	Commander in Chief Pacific
COA	Course of Action
COG	Center of Gravity
COMUSSAG	Commander U.S. Support Activities Group
CONOPS	Concept of Operations
COPS	Current Operations
CSO	Company Security Officer
CTF	Combined Task Force
DON	Department of the Navy
ECOA	Enemy Course of Action
EMIO	Extended Maritime Interdiction Operations
ESDP	European Security and Defense Policy
EU	European Union
FCC	Fleet Command Center
FOPS	Future Operations
FTE	Full Time Equivalent
GEO	Geo-Synchronous Orbit
GPS	Global Positioning System
GRT	Gross Registered Tons
HOA	Horn of Africa
HF	High Frequency
IMB	International Maritime Bureau

IMO	International Maritime Organization
INMARSAT	International Maritime Satellites
IPOE	Intelligence Preparation of the Operational Environment
IRTC	Internationally Recognized Transit Corridors
ISE	Intelligence Support Element
IW	Indications & Warning
KIM	Knowledge and Information Management
LEO	Low Earth Orbit
LRC	Logistics Readiness Center
MIOC	Maritime Intelligence Operations Center
MOC	Maritime Operations Center
MPG	Maritime Planning Group
MSC-HOA	Maritime Security Center Horn of Africa
MSPA	Maritime Security Patrol Area
MV	Motor Vessel
NAVCENT	United States Naval Central Command
NMCC	National Military Command Center
NATO	North Atlantic Treaty Organization
NPS	Naval Postgraduate School
NSC	National Security Council
OODA	Observe, Orient, Decide & Act
ONI	Office of Naval Intelligence
PLF	Palestinian Liberation Front
PLO	Palestinian Liberation Organization
PM	Project Manager
POW-ER 2.0	Process, Organization, Work for Edge Research 2.0
PRC	Piracy Reporting Procedure
RPG	Rocket Propelled Grenade
SL	Subteam Lead
SMS	Short Message Service

SNMG	Standing NATO Maritime Group
SOLAS	Safety Of Life At Sea Convention
SSAS	Ship Security Alert System
ST	Subteam Member
TFG	Transitional Federal Government
UIC	Union of Islamic Courts
USAF	United States Air Force
USCG	United States Coast Guard
USD	United States Dollar
USN	United States Navy
USS	United States Ship
UN	United Nations
USG	United States Government
VDT	Virtual Design Team
WFP	World Food Program

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The authors of this thesis would like to express sincere gratitude to our primary thesis advisor, Steven J. Iatrou, and co-advisor, Daniel F. Warren. We are especially grateful for the patience they showed as we completely shifted gears mid-thesis in how we wanted to approach our research. We appreciated the guidance and constructive criticism that allowed us to arrive in the end with a quality thesis. Additional thanks must be given to Dr. Mark Nissen and Dr. Douglas MacKinnon, for their introduction to and help with using the POWER modeling software, a key aspect of our research.

LT Christopher Descovich

Thank you to my wife, Christy, whose patience and support during the harpooning of this Monster.

To my son, Brendan (who likes pirates), thank you for always making me smile despite our most thunderous thesis storms.

To my thesis partner, Ryan, thank you for everything, not the least of which being a stress-free thesis partnership.

LT Ryan O’Connell

To my wife, Jennifer, thank you for your love and patience throughout this process. Thank you for stressing out about my thesis so that I did not have to. You have done a tremendous job managing both Mackenzie and me throughout our time here.

Thanks to my thesis partner, Chris thank you for what can only be described as a mellow and easy working environment.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OVERVIEW

Piracy is defined by the International Maritime Bureau as “An act of boarding or attempting to board any ship with the apparent intent to commit theft or any other crime and with the apparent intent or capability to use force in the furtherance of that act” (Dillon, 2005). Piracy thrives in ungoverned spaces and particularly in narrow waterways around the globe. The issue of cooperating with governments that either, permit piracy, behave ambivalently toward it or, worse yet, are powerless to act against it are the most complex of all. An increase in pirate attacks in the Gulf of Aden is only the most recent example of the impacts of piracy on the world’s commercial and private shipping industry. Legal issues, international coalitions, different geographic areas of responsibility and different reporting entities are all challenges to timely piracy reporting.

The response to incidents of piracy by governments and private organizations has been inconsistent. For insurance companies, it has been easier to allow the vessel to be taken, at which point ransom is then paid. Some governments have chosen to fight back against pirates, detaining pirates and destroying their property when opportunities present themselves, while other governments choose not to respond or remain powerless to do so. These inconsistent practices increase the response time of nation state forces sent to respond to singular incidents of piracy.

Commercially available technology could easily be integrated into U.S. Navy command and control architecture to alert anti-piracy assets before pirates board vessels and take crews hostage. Ship Security Alert Systems (SSAS) are required on all merchant vessels greater than 500 gross tons. When the alarm is triggered, current reporting procedures alert the home office of the company that owns the vessel.

Attention must be paid to the operational climate of any region in which piracy is an ongoing threat. Piracy is one of many warfare areas drawing on the resources of the Combatant Commander; this must be considered when forces are (notionally) allocated. The model in this thesis will attempt to show the amount of time each person in the

Command and Control organization will allocate to this mission. This thesis then intends to demonstrate that an organizational structure that facilitates a more streamlined reporting process, and commercially available technologies, can expedite a response from U.S. Forces.

B. GEOGRAPHIC BOUNDING

Piracy is a global problem; however, this thesis focuses on established Somali pirate areas of operation, to include the Gulf of Aden and the Indian Ocean. Focusing on this geographic area helps to frame the structure of the Department of Defense forces that monitor, assess, allocate forces and respond to piracy. For the purposes of this thesis, the scope of reporting procedures and organizational structures that support response to incidents of piracy is bounded geographically by U.S. Central Command's area of responsibility. As piracy is a maritime domain problem, U.S. Naval Central Command (NAVCENT) is the responsible agent for executing maritime operations in the waters surrounding the Horn of Africa. The Maritime Operations Center (MOC) at NAVCENT exists, "to streamline the operational cycle and to provide a structure for quickly and effectively establishing support for an operational level maritime commander" (Department of the Navy, 2008).

C. CURRENT CHALLENGES/THESIS INTENT

Piracy exists globally because it is an established criminal activity that preys upon slow moving merchant ships with little or no means of self defense. With more than 90% of the global trade moved by sea, modern piracy can be blamed for an estimated annual loss between 13 to 16 billion dollars world wide (International Maritime Organization, 2005). This thesis will focus on piracy in and around the Horn of Africa. Many factors are credited with the genesis of this modern pirate threat. Perhaps the largest contributing factor is the lack of a centralized government in Somalia with control throughout the country, though seven factors are cited that take a more precise look at the overarching reason, "Legal and jurisdictional weakness, Favorable geography, Conflict and disorder, Underfunded law-enforcement/weak security, Permissive political environments, Cultural acceptability and the promise of reward" (Murphy, 2009).

Exacerbating these environmentally permissive issues are the legal and industry standards of current international maritime shipping. Currently, the industry standard for reports of pirate attacks is to notify the International Maritime Bureau's (IMB) Piracy Reporting Center (PRC). This is completely voluntary, however, and no ship is required to do this beyond specific shipping company policy. The decision to report an incident of piracy and to request assistance to an incident of piracy is left up to the shipping company. The IMB states that its PRC "works closely with various governments and law enforcement agencies and is involved in information sharing in an attempt to reduce and ultimately eradicate this crime" (International Maritime Bureau, 2010).

The apparent reluctance to report these incidents stems from the number of organizations, corporate and state, involved in the shipping trade. There is no clearly delineated reporting chain for vessels operated by companies headquartered in foreign countries that do not hold the registration for that vessel. This has led to the reports of pirate attacks going to the PRC (which can take no action to stem the pirate scourge), and the shipping company executives who ask for help at their leisure. This process works only in terms of forewarning mariners of areas where the threat of piracy exists. It does little to combat the problem directly. This problem cannot be avoided simply by not going where the pirates are. This is because the cost to shipping companies to reroute ships longer distances increases the cost of operations and pirates have likewise have invested enough in their trade to expand their reach clear across the Indian Ocean. In March of 2010, the M/V Frigia was attacked and taken by Somali pirates more than 1,000 miles off the coast of Somalia. "That ship sailed through the dangerous zone in a convoy, escorted by (Turkish navy frigates) the Gediz and Gelibolu," a spokesman, Ayhan Ugurlubay, told Turkey's state-run Anatolia news agency" (Rice, 2010).

Reengineering large organizational structures such as the Department of Defense or Department of the Navy is difficult and the consequences of such a change may not turn out as they were envisioned. In the information age, technology changes to an organization's enterprise architecture can also have unknown consequences when changes to an organization's enterprise architecture are made. Small changes to an organization's C2 structure can give an organization a competitive advantage by

optimizing the speed at which an organization conducts business and optimizing force structure. The "As Is" process of piracy reporting is examined closely to find areas that are impediments to the flow of information. The "To Be" process looks to propose changes to areas discovered in the "As Is" process. This thesis proposes a small change in reporting structure and reporting technology can optimize force structure and the speed at which the Navy responds to an incident of piracy.

The NAVCENT MOC is the ideal candidate to directly receive information regarding an act of piracy to begin the process of supporting an operational level maritime commander in deciding courses of action to a specific incident. There are many vectors for notification by the Merchant ships. International Maritime Satellites (INMARSAT) is a technology shared by both the U.S. Navy and the commercial shipping industry to enable the exchange of e-mail for notification of pirate attack. The use of commercial satellite phones also enables merchant ships to call for help. Another emerging technology is the Ship's Security Alert System, which transmits text and SMS messages to whomever the company directs. This thesis proposes that this technology will greatly improve the speed with which U.S. naval forces are notified when merchant ships are required to report direct to a MOC. The authors test this hypothesis through computer based experimentation using POW-ER software.

Current reporting procedures have proven legally expedient, but experience significant time lag both in the physical act of the report as well as notification between various agencies with the U.S. government. This time lag is unacceptable when the default response is the sortie of U.S. military forces independent of the amount of time provided for appropriate planning and execution of operations. Small changes to Command and Control functions in the existing reporting system can lead to the construction of a new framework optimizing forces on station while maximizing time to respond. While the United States cannot require foreign flagged vessels to report attacks to the U.S. Navy, the U.S. Coast Guard can require U.S. flagged ships to report attacks as a part of the vessels' annual Certificate of Inspection. The intent of this thesis, however, is to postulate the benefits of using the Ship's Security Alert System (SSAS) by U.S. flagged merchant ships directly reporting to U.S. Navy's 5th Fleet Maritime Operations

Center. By answering the questions below, the authors believe this to be one practical way to give the advantage to U.S. military forces operating in a dynamic environment spanning millions of miles of ocean.

1. Which is the optimal method for reporting incidents of piracy that will minimize response time and increase the probability of disrupting the event before it becomes a hostage/ransom situation?

2. What changes to the command and control structure provide for mission optimization and optimization of forces in theater?

D. ASSUMPTIONS

1. The procedures represented in the model as well as the interactions between the positions are derived from the U.S. Navy's MOC Concept of Operations NTTP 3-32.1

2. There is an existing legal requirement by USCG for U.S. flagged merchant ship to report pirate attacks to a numbered Fleet's MOC.

3. The entire response to these attacks will be coordinated and executed unilaterally by U.S. forces.

4. SSAS technology is mature and compatible with existing U.S. Navy networks for seamless implementation.

5. The results generated by the POW-ER model are statistical approximations.

6. The model used has complete cooperation with the shipping company through its representative (Company Security Officer) in all scenarios.

E. CHAPTER OUTLINE

Chapter II of this thesis is a historical review of U.S. government response to incidents of piracy throughout history, an in-depth look at Somali pirate groups to include their Command and Control structures and a technology review of Ship Security Alert System. Chapter III introduces POW-ER 2.0 software as a tool for modeling piracy reporting procedures as they exist today and proposed changes to those procedures that

may decrease the time it takes to respond to an incident of piracy. Chapter IV will include running the POW-ER 2.0 software simulations. The results from these simulations will be contrasted between the "As Is" reporting procedures to the "To Be" reporting procedures. Analysis of these results will build the foundation for the recommendations in Chapter V. Chapter V will supply recommendations for future areas of research and conclude this thesis.

II. BACKGROUND

A. THE TROUBLE WITH PIRATES

1. Overview

The challenge of protecting U.S. commercial interests at sea has always been at the core of the United States Navy's mission set. The first six frigates commissioned after the Revolutionary War were built specifically to counter the threat of piracy. It is no surprise, then, that today's Navy would have a keen interest in combating piracy as it is responsible for 13 to 16 billion dollars in annual losses to worldwide maritime trade. Effective Command and Control of the forces assigned to combat piracy is essential to how planners craft their various responses to emergent situations.

How then are today's advanced reporting techniques best exploited by U.S. Navy C2 processes within a Maritime Operations Center? Command and control is defined by Joint Publication 1-02 as, "the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission" (CJCS, 1995). The Navy's MOC will establish a centralized C2 mechanism applying the principles outlined in the joint publication on C2 processes. Applying these principles will lay a foundation from which to achieve effective command and control.

Without effective command and control, emergent incidents of piracy in remote oceans around the globe can have disastrous consequences. The issue of maritime piracy offers an example of an emergent situation that requires rapid, accurate notification of events, and a clearly delineated means of dealing with the threat. The United States Navy is charged, among other things, with maintaining sea routes to aid the movement of

commercial shipping, which supports the United States' and global economies. History offers several dynamic examples of command and control approaches to draw from to combat piracy.

B. PIRACY THROUGH U.S. HISTORY

1. Barbary Corsairs

The U.S. response to piracy off the coast of North Africa in the early 1800s was the result of U.S. merchant ships being taken by pirates from the Ottoman Empire backed nations of Algiers, Tunisia and Tripoli.

In the 1790s and into the 1800s, the business model was simple and effective for the Barbary Coast nations. Capture of foreign merchant ships provided a source of income and labor as the crew of the vessel was forced into labor until ransomed by their native country. In the 1790s, the U.S., having no navy, could do little but pay tribute to Algiers to prevent taking of U.S. merchant ships. In August of 1812, a U.S. merchant ship, the brig *Edwin*, was taken by an Algerine Frigate. Few details are available about the chase and capture of the *Edwin*, however.

> The pursuer, a frigate armed with two rows of cannon on her broadside, overhauled the Edwin. Although no account exists of the chase and capture of the Edwin, the scene was played out hundreds of times in that era, and there is little doubt of the essentials. As the distance closed, the pursuing vessel might have hoisted a green banner with white crescent and stars, the flag of Algiers, or she might have dispensed with identifying herself and fired a single cannon shot across the bow of the Edwin, the timeless display of force meant to be answered by force or submission. The unarmed Edwin must have heaved to, backing her topsails to stop and submit, as a boat put off from the Algerine frigate loaded with men. Rowed over to the Edwin, they would have clambered up her side armed with swords and pistols and, shrieking threatening words in Arabic, taken control of the brig. The crew of the Edwin, overwhelmed and unnerved, insulted and spat upon, surrendered. (Leiner, 2006)

Events building up to the capture of the *Edwin* show that several breakdowns in command and control certainly contributed to her capture and the subsequent enslavement of her crew in Algeria. The crew of the *Edwin* had been hailed at sea five years before the Algerine boarding by a French Privateer in the Atlantic in 1807. The

Frenchmen were content to only ask for a top mast and then left the *Edwin* to go on her way (Leiner, 2006). Perhaps the crew of the *Edwin* expected a similar outcome in August 25, 1812, with the Algerine frigate.

The new U.S. government had difficulty in trying to reach all civilian merchant shipping prior to declaration of war against Great Britain. The *Edwin* and her commander Master George Campbell Smith landed at Gibraltar and then Malta on June 29, 1812, where, “Neither British authorities ashore nor Master Smith could have known…that exactly eleven days earlier the United States had formally declared war against Great Britain” (Leiner, 2006).

On August 5, 1812, the *Edwin* departed Malta under Royal Navy Convoy on her journey home. Due to poor sailing practices the *Edwin* lost the convoy one evening and was forced to sail alone (Leiner, 2006). Without the protection of the convoy the *Edwin* was in a very vulnerable position sailing the waters of the Mediterranean with no means to defend the ship against pirate attacks. The *Edwin* was taken on August 25, 1812 and arrived in port at Algiers a few days later. The first notification of the incident reached the U.S. Consul at Gibraltar in November 1812. The United States had no forces to respond to the seizure of the *Edwin* in the Mediterranean and any forces available were thousands of miles away and could take months to arrive. Nine months passed before President Madison would dispatch a representative to negotiate the release of the captured crew in Algiers.

Unlike present day, which is marked by high tech means of communications, the early 1800s saw communications move by word of mouth or letter dispatched by sail or horseback. In the age of sail, ships could be expected to average eight knots consistently. Given the distances required for information to travel, letters of notification would obsolesce en route, preventing a coordinated response outside of local on-scene commanders patrolling the waters of the Mediterranean. With no forces in the Mediterranean, the United States was initially forced to the negotiating table, which forced several trans-Atlantic passages moving at eight knots to come to agreeable terms.

The capture of the brig *Edwin* ultimately evoked a military response by the U.S. Navy. Already paying protection money to the Dey of Algeria and incensed that Algeria would still take U.S. merchant shipping as plunder, inspired the deployment of two squadrons at the order of President Madison to then Secretary of the Navy Crowninshield. Commodore Stephen Decatur was to command the first squadron and Commodore William Bainbridge the second. Decatur's squadron was to depart first, and in large part the success of his mission was due to the clear orders given to him prior to departure for the Mediterranean and the conflict with Algeria. His orders from Secretary of the Navy Crowninshield highlight how command and control through commander's intent were used effectively to accomplish the mission.

Figure 1. Barbary Coast (From Malte-Brun, 1829)

Decatur's orders were issued on April 15, 1815, "The orders authorized Decatur to subdue, seize, and make Prize of all Vessels, goods & effects belonging to the Dey or subjects of Algiers, even as Decatur was to endeavor to capture or destroy any Algerine cruisers that he encountered" (Leiner, 2006). Decatur was given clear orders as to what

his mission was, how his commander's envisioned the end state of the mission but Decatur was given considerable latitude in how to accomplish that mission given that communications in the age of sail were slow.

Dispatching forces locally to the waters of the Mediterranean was necessary to carry out the commander's intent. Given the speed and frequency of pirate attacks distance between Decatur and Jefferson would not allow for day to day oversight of the operations of the Mediterranean Squadron. Due to the fact that communications could take months to travel from the Mediterranean back to the United States, Decatur had to have a clear idea of what the mission would be in order to organize his forces and commit them to the fight effectively. The orders issued by the Secretary of the Navy were explicit enough on who the war was with and what the expected outcome of the war would be; it was up to Decatur on how he would use his squadron of ships to fight Algerine ships.

Figure 2. Decatur's action against the Philadelphia (From Fraser, 1920)

As Decatur sailed into the Mediterranean his understanding, although not described in the same way as today, of the command and control process turned into a victory against several Algerian ships including the defeat and death of Algeria's most decorated admiral, Reis Hammida, which proved to be powerful bargaining chips to the

Dey of Algeria helping the United States in its political negotiations with Algeria. The Observe, Orient, Decide and Act or OODA loop can be applied to Decatur's campaign in the Mediterranean in the summer of 1815 and his successful taking of an Algerine frigate Mashouda and an Algerine brig Estedio. Information fuels the C2 process, in the case of Decatur's Mediterranean squadron he set out to gather quality information about the location of Algerine ships sailing alone, especially a command ship. Decatur learned from the American consul at Cadiz that an Algerine squadron was active in the Mediterranean and later confirmed that intelligence with the consul at Tangier. Decatur further fueled his understanding of the situation when at Gibraltar he received information that the Mashouda and Admiral Hammida could be found off of the coast of Spain waiting to receive tribute payment from the Spanish Government (DeKay, 2004). This information allowed Decatur to dictate the terms of the situation to the Algerians by allowing him to act before his adversary.

Decatur's presence in the Mediterranean allowed him to match the speed of operations the pirates of Algiers were operating at, in this case approximately 8 knots. With forces positioned in the operating area interdiction of pirates became realizable. Operating under a clear commander's intent prevented delay in operations allowing Decatur to capitalize on time sensitive information and battlefield successes.

The gathering of accurate, relevant information helped Decatur achieve understanding of the situation. In this case the understanding that if part of his mission was to capture Algerine ships, the capturing of arguably one of the most important Algerine ships, that of Admiral Hammida, would affect the Algerian's OODA loop extensively. Decatur meanwhile observed, through the gathering of information, that there was in fact an Algerine squadron active in the Mediterranean, oriented himself to the fact that it was a flag ship commanded by Algeria's greatest Admiral, decided he would find and attack it and acted upon that decision when the American squadron found the Mashouda 20 miles off the coast of Spain. Effective command and control aided in the success of Decatur's Mediterranean squadron leading to new treaties with the Barbary states in which the United States no longer would pay tribute. This resulted in the United States adopting a policy of countering and deterring piracy through forcible means.

2. The *Mayaguez* Incident

On 12 May 1975, the U.S. flagged MV *Mayaguez* was attacked and seized in the vicinity of the Poulo Wai Islands. Although there is debate about whether or not the taking of the U.S. merchant vessel *Mayaguez* was an act of piracy there is no doubt that it was an emergent crisis situation at sea. The incident involved a U.S. flagged merchant vessel and its crew being interdicted and boarded by a Cambodian gunboat. The following is outside support claiming that the *Mayaguez* incident was an act of piracy. In the Naval War College Newport Papers titled Piracy and Maritime Crime: Historical and Modern Cases author of Chapter Four Charles Koburger Jr. includes the *Mayaguez* incident as a well known example of piracy in the South China Sea (Koburger, 2010). Additionally, shortly after a meeting with his National Security Council (NSC) regarding the taking of the *Mayaguez*, then President Gerald Ford, "issued a press release declaring the seizure an act of piracy, holding the Cambodian Khymer Rouge government responsible" (Guilmartin, 1995).

Shortly after the fall of Cambodia to the Communists on 17 April 1975 and similar incident unfolding in Vietnam on 30 April 1975, the incident of the Merchant Vessel *Mayaguez* would unfold. On 12 May 1975 approximately six and half miles from the Poulo Wai Islands the *Mayaguez* was seized by Cambodian gunboats (Paust, 1976). The *Mayaguez* was steaming from Hong Kong to Sattahip, Thailand. The Cambodian gunboat approached the *Mayaguez*, which was steaming at 12.5 knots and with a boarding party from the gunboat took control of the *Mayaguez*, it was 1421 local time and 0321 in Washington, D.C. (Guilmartin, 1995). U.S. military reconnaissance assets were providing aerial reconnaissance of the situation hours after the incident unfolded providing the chain of command with their interpretation of events unfolding on the seas below them.

The fact that the *Mayaguez* was a U.S. flagged vessel gave the USG the speed to begin planning immediately on reclaiming the ship through diplomatic means or military force. The response time would have been much longer had the vessel been flagged under a different country and had a foreign crew aboard because input would have to be

gathered from those foreign governments on how to proceed with reclaiming the vessel. Similar to the era of the Barbary Pirates the United States was able to act unilaterally against hostile states attacking their merchant ships.

It is important to understand how and when the U.S. government was notified of the incident that would provide it with the information to respond with a joint military effort. It is also important to consider that many advances in military technology especially weapons technology were at the disposal of responders to the *Mayaguez* crisis. “But the advent of actual world-wide communications, offering national leaders the possibility of immediate control of military forces on a global basis, was surely among the most important” (Guilmartin, 1995).

Minutes prior to the seizure of the *Mayaguez*, crew members transmitted, “an SOS in Morse Code on standard maritime distress frequencies…” and “then broadcast an emergency message in the clear on HF (high frequency) voice radio” (Guilmartin, 1995). A Mr. John Neal received the SOS at 0718 Zulu (Z) hours in Djakarta, Java working for the Delta Exploration Company (Guilmartin, 1995). The transmission picked up by John Neal from the *Mayaguez* is as follows: “Have been fired upon and boarded by Cambodian armed forces at 9 degrees 48 minutes north/l02 degrees 53 minutes east. Ship is being towed to unknown Cambodian port” (Office of the Joint Seceratary, 1976).

Figure 3. Map of Kaoh Tang Island (From Commons, 2010)

John Neal relayed this information to the U.S. Embassy also in Djakarta, Java. Two hours after the U.S. Embassy receipt of the SOS message it was relayed to Washington, D.C. After word of this moved up the chain of command in Washington, "At twenty to eight in the morning eastern daylight time, President Gerald Ford was notified by Lt. Gen Brent Scowcroft, USAF…just over six hours had elapsed since the *Mayaguez* transmitted her SOS" (Guilmartin, 1995). At 1205, a meeting of the National Security Council was called the outcome of which set in motion the use of military force when diplomatic efforts proved to be ineffective in trying to secure the release of the *Mayaguez* and her crew. Six hours after the *Mayaguez* was taken, the information had reached the President of the United States' desk, and initial planning for the retaking of the *Mayaguez* was laid down.

When a pirate attack occurs, swift notification is critical to begin developing courses of action and well-established lines of communication are critical to directing forces to be utilized in any operations against a pirated vessel. The fact that communications moved so swiftly enabled the USG to interdict and prevent the *Mayaguez* from being towed to Kompong Som and well within Cambodia's territorial

waters. The speed at which communications traveled at the time was an advantage only if the C2 structure for disseminating operational orders was in place. This is evident in two instances with the *Mayaguez*.

The first instance is the information flow that alerted President Ford that the *Mayaguez* was taken. The reporting scheme was a series of relayed communications that took six hours from distress signal to notification of the President. Had the distress signal gone to a designated contact within the USG or military to handle such events, relay upon relay of the information, which proved to be time consuming, would not have occurred. The planning process by President Ford and his staff did not occur until six hours after the ship was taken.

The second instance was the C2 structure and subsequent information flow that would direct U.S. military forces to retake the *Mayaguez*. After deliberating on courses of action, late in the day of the 13^{th} and into the 14^{th} the order had been given to use force to prevent the *Mayaguez* from being towed to the Cambodian mainland port city of Kompong Som. The communications apparatus in this instance was critical in relaying information to U.S. decision makers to begin developing a course of action for how to respond to the seizure of the American flagged vessel and coordination of forces involved in the operation to recover the *Mayaguez*. The communications links and nodes are illustrated from top to bottom below.

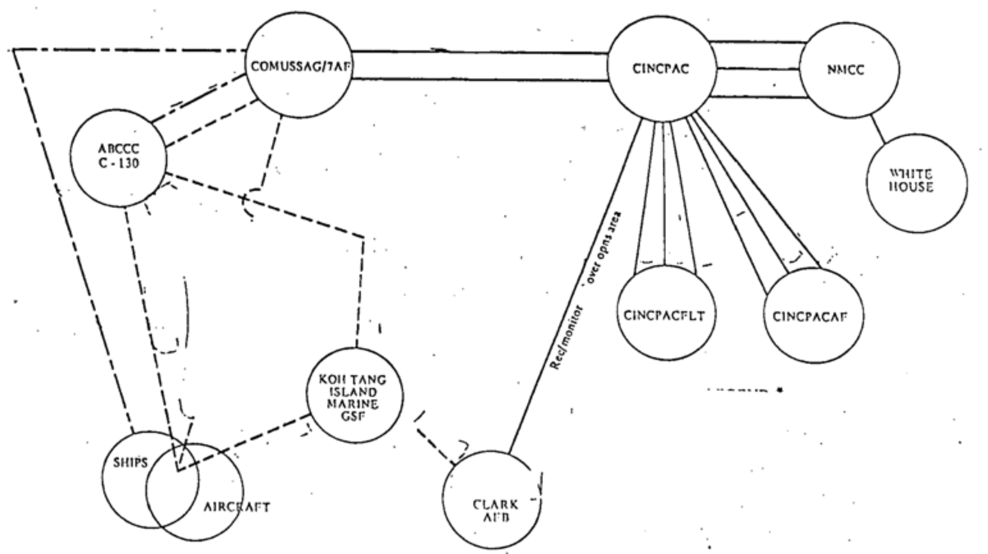

Figure 4. Communications for S.S. *Mayaguez* response/Kaoh Tang Operation (From Office of the Joint Seceratary, 1976)

Operational command of forces on scene was given to Commander U.S. Support Activities Group/7th Air Force (COMUSSAG/7AF). Upon being established as the on-scene commander COMUSSAG/7AF released the following message, "…The international implications of this operation make restraint imperative. Complete command and control must be maintained by COMUSSAG/7AF, who will be acting upon direction from the National Military Command Center…" (Office of the Joint Seceratary, 1976). The selection of one on-scene commander enabled all operational forces to be leveraged in a cohesive unified way. Below is an excerpt from the after action report of the *Mayaguez* incident detailing objectives for COMUSSAG/7AF to accomplish. The efficiency of communications and clearly delineated C2 structure enabled a chain of command to be established that was able to communicate a plan to superiors for approval and then disseminate that plan to subordinates for action. With a plan in place:

> Just before one o'clock in the morning of 14 May, CINCPAC and USSAG/7AF were tasked by the Acting Chairman, following an NSC meeting, to make preparations to seize the MAYAGUEZ, occupy Kaoh Tang Island, conduct B-52 strikes against the port of Kompong Som and Ream Airfield, sink all Cambodian small craft in target SEA. Preparations were to be completed in time for execution early on 15 May. The

> USSAG/7AF concept plan to conduct these operations was received in Washington at 1330 hours on 14 May and approved, with minor modification, by CINCPAC. The operational concept is attached at Tab C and subsequent events followed this scenario closely, with tactical air from the USS CORAL SEA being substituted for B-52's in the attacks on the mainland. (Chairman of the Joint Chiefs of Staff, 1975)

All of these objectives were accomplished, by 0025 EST on 15 May the crew had been recovered and returned to the *Mayaguez* and the *Mayaguez* was being towed by the USS Holt. The response to use military force to recover the *Mayaguez* and crew can be viewed as a success from the perspective that at the end of the operation the crew and the vessel were recovered. Although not knowing the exact location of the crew led to unnecessary operations on Kaoh Tang Island, one dedicated on-scene commander with clear objectives enabled forces to be leveraged in such a way that a successful interdiction of the pirated vessel was possible. Additionally, the speed at which communications was able to flow enabled the United States to respond to the incident before the Khmer Rouge could decide its next step after taking the crew and the *Mayaguez*.

Figure 5. U.S. Marines maneuvering aboard the *Mayaguez* (From American Merchant Marine at War, 2000)

3. The *Achille Lauro*

The Palestinian Liberation Front (PLF) attacked the *Achille Lauro* in 1985; this attack serves as an example of the disastrous consequences of a crisis situation at sea where the command and control process breaks down, complicated by the necessity to

coordinate with foreign nations. The capture of the *Achille Lauro* was unique in that the ransom demanded by the PLF was “political prisoners.” It is a valid case study, however, given that regardless of the demands, four armed men took a ship to ransom passengers and crew. The *Achille Lauro* was boarded and taken on 7 October 1985 by four armed members of the aforementioned PLF. Notification of the attack came when the PLF members issued their initial demands to the Italian government. The response by the United States shows the quantum leap in technology between the Barbary wars and 1985. By the time night fell on Washington, D.C.,

> Groups consisting largely of top brass who had handled the TWA hijacking were being hastily convened in Washington, with lines of communication to President Reagan. An emergency team of experts in counter-terrorism and communications was sent to Rome to advise the U.S. ambassador there. Special forces (the Delta Force) were sent on their way from their base in North Carolina to a NATO airbase in Sicily. (BBC, 2002)

Meanwhile, the Italian government was drawing up plans for a response in parallel but independent of U.S. plans, the *Achille Lauro* being Italian flagged gave authority to retake the ship to the Italian government. Upon learning that passenger Leon Klinghofer, an American citizen on a wheelchair, was thrown overboard to his death, President Ronald Reagan changed the overall tack for responding to the incident, from one of observation to planning for direct action. Despite modern satellite surveillance techniques, no system for reporting incidents of piracy at sea had been developed to allow tracking of the *Achille Lauro*. The ship went completely undetected until an Israeli patrol boat stumbled upon her and reported her position to the United States

> From then on the *Achille Lauro* was followed by three vessels of the U.S. navy in a position to launch an attack. U.S. diplomats in Rome and Cairo were trying to avoid negotiations with the PLF and keep the ship outside Egyptian territorial waters. But the Egyptian government was happy to allow her to enter its waters in spite of U.S. opposition. (BBC, 2002)

Though Somalia does not have recognized territorial waters, forces operating in an anti-piracy role have largely respected the 12-nautical-mile buffer surrounding Somali shores. This casts a brighter light on the legal precedence for prosecuting acts of piracy around the Horn of Africa.

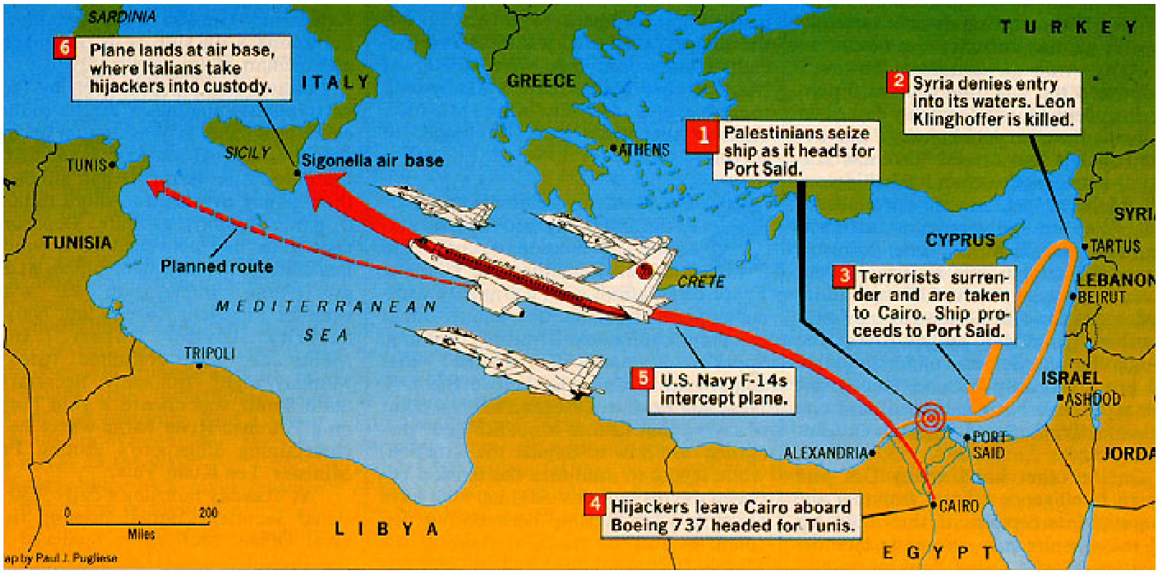

Figure 6. The Flight path of the PLO hostage takers (Elliott, 2009)

By 9 October 1985, the *Achille Lauro* was anchored in Port Said and the hijackers had agreed to hand over the hostages under the pretense that they would in turn be handed over to the Palestinian Liberation Organization (PLO) to stand trial. This angered the United States, which to this point had not had to use any force to resolve the situation. However, the Egyptians wanted the PLF members out of the country and to be done with the whole ordeal, they wanted to fly the men to either Italy or the United States. Yasser Arafat wanted the hijackers turned directly over to him. While the plane was in the air, "F-14s from USS *Saratoga* (CV-60) intercepted an airliner bearing the men and forced the plane to land at a U.S. base in Sicily, where they were turned over to Italian authorities" (Department of the Navy, 2000). The U.S. Navy had many new high-speed tools in its maritime response tool kit. While the initial response to deploy forces to the scene and the information flow when forces had arrived moved quickly, technological advances played no large role in resolving the crisis. Fortunately for all those aboard the *Achille Lauro*, the turnover of the ship and hostages was realized before an assault on the ship had to take place.

4. The Maersk *Alabama*

Perhaps the most relevant incident of piracy in recent history is the case of the MAERSK *Alabama*. The attack on the *Alabama* clearly demonstrates the willingness of Somali pirates to attack and hold U.S. flagged merchant ships. The actions taken by the crew created unique aspects to the scenario but ultimately the attack resulted in the same hostage at sea situation that has become the modus operandi of pirates operating around the Horn of Africa. The attack on the *Alabama* started on the 8 April 2009, but crewmembers actually report sighting two small boats at range of "two miles continuing to advance" the day before (Marine Officer, 2009).

The sea-state prevented pirates from successfully attacking the *Alabama* on 7 April; however, the seas were like glass on the eighth. After several hours of attempting to evade the pirates, the container ship was overtaken by the pirates. Once the pirates closed to one mile, Captain Phillips (the master of the *Alabama*) sounded the general alarm (Marine Officer, 2009).

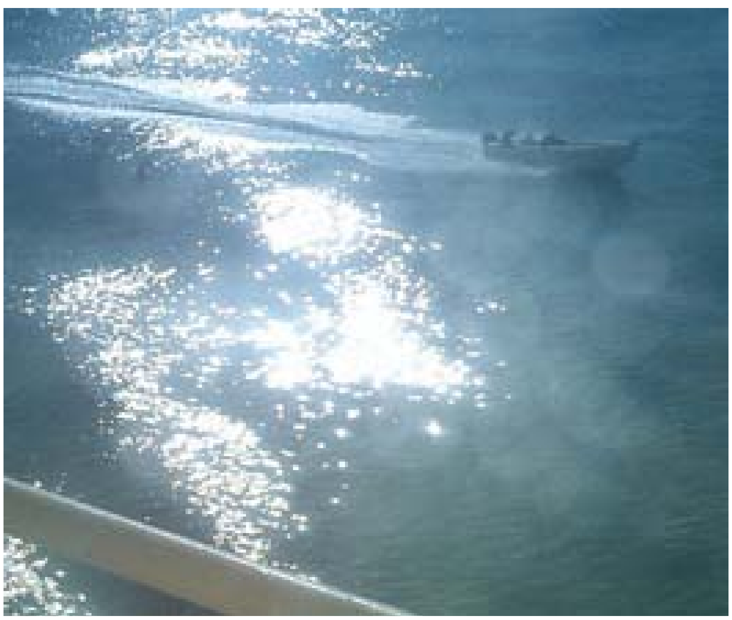

Figure 7. Photo of pirates shortly before boarding 08 APR 2009 (From Marine Officer, 2009)

The Navy was notified of the situation late in the day on 8 April by the MAERSK Corporation (Weaver, 2009). The Navy dispatched the *USS Bainbridge* in response. The

Bainbridge, located some 300 nm from the site of the attack when first notified, reaches the *Alabama* at approximately 0300 local time on 9 April. The *Bainbridge* arrived on the scene to find all four pirates and Captain Phillips in one of *Alabama's* lifeboats. A botched hostage exchange between the merchant crew and the pirates left the captain with food and water but still in the hands of four hostage takers.

Figure 8. The 28-foot lifeboat where Captain Richard Phillips and the four Somali pirates were held up, as seen from a U.S. Navy Scan Eagle UAV (From Weaver, 2009).

A wounded pirate was transferred to the *USS Bainbridge*. He then attempted to broker a deal between the remaining pirates and U.S. forces. The lifeboat was then taken under tow by *Bainbridge.* The Commanding Officer of *Bainbridge* had been given permission to use deadly force if Captain Phillips was deemed to be in imminent danger. Then on Sunday, 12 April 2009, U.S. Navy SEAL sharpshooters performed three simultaneous shots, killing the three pirates on the lifeboat instantly (Marine Officer, 2009). Similar to Decatur's actions on the authority of the president, the actions on the part of the *Bainbridge*'s Commanding Officer is a modern-day example of a lower-level commander carrying out his commander's intent to counter an act of piracy.

C. FACTORS CONTRIBUTING TO PIRACY

1. Pirates At Sea, Patriots At Home

The dynamic of modern piracy has changed. Before, strong regional powers stole from foreign countries that were so far away they seemed powerless to upset the status quo; now, local thugs steal in an attempt to force the economies of the world's most powerful nations to bend to their will. The political climate in the central region of Somalia lends itself well to piracy, a partition with one of the leaders referring to international forces as "a "bunch of amateur tourists" who, by systematically conceding to the pirates' blackmail, are supporting their flourishing industry" (Quérouil, 2008). During the blockade and standoff with Motor Vessel Faina, local leaders proposed the idea of simply bombing the ship and neutralizing both the pirates and its military cargo. This idea did not appeal to the international community, given the civilian crew still being held aboard the ship. This fundamental difference in approaches highlights just some of the cultural differences in the parties involved.

It is often argued that the solution to piracy will be found on land, through sorting out the political mess that has kept Somalia in turmoil for nearly 20 years (Bahadur, 2009). This means that simply landing forces and dispensing of the pirates in their havens may rid the Somali coast of its current threat but does little to solve the problem in the long term. As pirate successes mount, the pirate gangs become more entrenched in Somali society. As the reigning local entities, they have the money and power to feed and protect the local populous. The pirates are running local convenience stores, and mothers campaign to marry their daughters to pirate gang leaders—a crude yet lucrative stock exchange that trades in all the commodities required to send the pirates out on their missions. The pirates claim they are the "Savior[s] of the Sea" (Bahadur, 2009). As Somalia languishes in political and economic turmoil, few people living in Somalia can refute this claim.

2. Actors

It is important to know and attempt to understand the actors involved in modern day piracy; this understanding can offer solutions to piracy problem beyond responding to individual criminal acts that cost the global maritime trade billions of dollars annually. There are two schools of thought regarding the organization of Somali pirates; the first being one interconnected network of pirates committing coordinated attacks throughout the Gulf of Aden. The second school of thought is three regionally bound networks of locally controlled pirates projecting their sea-power from their northern, central and southern "pirate havens." Given the lack of infrastructure and the nomadic tendencies of the indigenous people, the authors of this thesis will proceed under the assumption that the three Somali pirate clans operate independent of each other.

The Northern clan is headquartered in the town of Eyl, pirates cruise the streets of Eyl and neighboring Garowe in new 4x4s and live in the relative lap of luxury. Jay Bahadur, a reporter from the *Times* of London, had the opportunity to interview Boyah, a man who claims to be the leader of the Northern Pirate clan. Boyah is one of the "Old Boys," a group of men who were raiding merchant ships long before Somalian piracy was the glamorous trade it is today. When asked by Bahadur whether or not Boyah considered himself a "burcad badeed" an "ocean robber," Boyah clarified that he was in fact a political "Savior of the Sea." Boyah further jokes that he is the Chief of the local Coast Guard. Though Boyah does seem to understand that what he is doing is wrong, he says the solution to the piracy situation lies in the hands of the international community and its efforts to restore the fishing grounds off the Somali coast.

He claims that the targets he and his men strike are "a legitimate form of taxation levied in abstentia on behalf of a defunct government that he represents in spirit, if not in law" (Bahadur, 2009). Boyah's business model seems to be working; he claims to have received $800,000 in ransom for a single target (Bahadur, 2009). Further, he claims to have 500 men working in the loose federation that is his pirate clan. He claims to be the clan's chief organizer, recruiter, financer and mission commander. Boyah claims that everyone who seeks the position of pirate must see him and swear allegiance until death, natural or otherwise. This leads to low turnover within the group.

Boyah estimates that roughly 20–30% of attacks are successful—not a very high success rate when Boyah himself admits his group targets anything that looks promising. Given the quality of life in Somalia, the relative fortunes doled out by insurance companies, and the development of a pirate commodities stock exchange, the modest success rate more than pays for the pirate's failures. Once a ship is captured:

> (It is) steered to Eyl, where guards and interpreters are brought to look after the hostages during the ransom negotiation. Once secured, the money—often routed through banks in London and Dubai and parachuted directly on to the deck of the ship—is split: half goes to the hijackers, a third to the investors who fronted cash for the ships and weapons, and 20 per cent to everyone else, from the guards to the translators (occasionally high school students on a summer break). Some money is also given as charity to the local poor. (Bahadur, 2009)

This has given Boyah the appearances of being a modern-day Robin Hood.

When Bahadur pressed Boyah about the training and techniques employed by his clan, he eventually admitted that many of his men were at one time Somali Coast Guard recruits. Somalia attempted in 1999 to establish an official Coast Guard to protect fisheries whose depletion had driven Boyah and many like him to a life of piracy. The official Coast Guard, however, soon broke down into gun-for-hire protection of local fishermen. When this system of "protection" broke down, a new generation of better trained pirates with more sophisticated weapons appeared (Bahadur, 2009).

In 2008, Manon Quérouil a freelance journalist, had the opportunity to interview Abdul Hassan the 39-year-old purported leader of the central region pirate clan leader. This clan goes by the name the "Central Region Coast Guard" (Quérouil, 2008) and operates out of the central city of Hobyo. The relatively young group was formed only three years ago, yet has attacked some 29 ships and received an estimate ten million U.S. dollars in ransom. Abdul Hassan claimed in his interview to have personally received $350,000 for his work. The relative opulence of these pirate successes is not hard to find in the city of Hobyo.

The Central Region Coast Guard claims to employ 350 men and operate over 100 speed boats. Hassan claims his men are a mix of former fishermen and disenchanted

militiamen. Hassan says that he himself was in fact a legitimate fisherman only a few years ago. He, much like his comrades in the North, attributes the drive to piracy to the overfishing of Somali waters by commercial fishermen.

The techniques of the pirates operating out of the central region of Somalia practice some of the most advanced pirate techniques. They often deploy their high-speed boats from larger mother ships, the entire attack may take as little as 15 minutes (Quérouil, 2008). The pirates also show their technical and navigation savvy by employing GPS to coordinate multi-boat attacks on their targets.

Harardhere is the homeport to the southern clan of pirates which also believe they are Coastguardsmen. Located 180 miles north of Mogadishu, Harardhere has always maintained a rough reputation. The popular saying in Somalia is "When in Mogadishu you have to earn your money, when in Harardhere just use guns" (Mojon, 2009). It is no surprise, then, that Harardhere is considered to be the birthplace of modern piracy. Stig Jarle Hansen a Norwegian researcher explains "Harardhere provided the perfect base for the pirates as it was far away from the fractions in the Somali civil war" (Mojon, 2009). This was important because it meant that the money Abdi took from ransom was his and his men's without having to pay tribute to local militias.

Though these clans claim to be small regionally bound entities their tactics seem to mirror one another. Whether this can be attributed to the training of the now defunct Somali Coast Guard or merely the identification of soft targets is a matter for future study. What is relevant, however, is that the attacks that make the evening news are not necessarily reflective of the majority of pirate operations in the Gulf of Aden.

3. Piracy as a Business Model

The business model for Somali piracy was established by Mohammed Abdi back in 2003–2004. Abdi was no sailor; he was (then) a mere bandit. He was educated in his seafaring trade by underlings he hired to help him. Abdi has, however, come a long way in five years. He has earned a spot on a UN watch list for violation of weapons embargoes. It is also rumored that he was briefly a member of al Qaeda and was seen at

a celebration in Libya marking Moamer Gathafi's 40 years in power. The Union of Islamic Courts even tried to have him hanged but failed when they were ousted in 2006.

The pirates have begun to use their newfound fortunes (estimated to be in the tens of millions of dollars (Ahmed, 2009) to create a stock exchange to fund future pirate operations. So far, this type of investing is contained to Harardhere. The investors are not limited to those who take to the sea themselves. It seems the "market" is a response to managing the investment of Somalis looking to earn money from piracy without having to commit the act.

One man named "Mohamed" claimed to be at least part of the creative force behind the stock exchange. Mohamed, a former pirate claims to support "72 ventures in the market and 10 which were successful" (Ahmed, 2009). He also said "The shares are open to all and everybody can take part, whether personally at sea or on land by providing cash, weapons or useful materials ... we've made piracy a community activity" (Ahmed, 2009). The stock exchange has become the center of Harardhere life not only to investors, but also to the sobbing family members inquiring, asking about news of missing loved ones who took to the sea.

While both pirates and equipment are lost at sea every week, investors are not deterred. This is due in large part to the dramatic increase in ransoms paid; ransoms have risen from $2–3 million U.S. dollars to greater than $4 million U.S. dollars (Ahmed, 2009); the increased demand promises many willing investors great returns on future ventures. One such investor is Sahra Ibrahim. She is a 22-year-old divorcee who bought a share in an attack on a Spanish tuna trawler. Her investment was a Rocket Propelled Grenade she received as part of her alimony. The return on this simple investment was $75,000 in a mere 38 days (Ahmed, 2009).

D. THE EFFECT OF MODERN PIRACY

1. Which Ships Are at the Greatest Risk?

Although large container ships, and those carrying vast military cargoes, rise to prominence once taken, it is the smaller ships, on the order of less than 1000 Gross Registered Tons (GRT), that are statistically at the most risk. Ships either anchored or moored pier-side are also among the pirates' favored targets (Murphy, 2009). This is for the obvious reason that a stationary ship is easier to board. In an Office of Naval Intelligence (ONI) study, attacks on moored ships were successful 90% of the time while attacks on ships underway were successful only 62% (Murphy, 2009).

Ships are still at risk while underway however, the most common method of attack is a small, fast, highly maneuverable boat approaching the target's stern. In some cases this is preceded by other similar boat harassing the forward portion of the target ship and distracting the bridge watch-standers. This harassment can come in many forms, ranging from the small boats crossing bow wakes to AK 47 staccatos and RPG fire at the target's wheelhouse. These methods are far superior to the fire axes and flaked out hoses that seem to have become the universal anti-piracy tactic. Larger merchant ship can afford more advanced security systems that include electrified railings and security doors that are controlled by electronic locks. These systems do little however for small merchant and fishing vessels who find themselves at the greatest risk anyway. Due to insurance policy stipulations and restrictions of ports on ships that enter make the carrying of fire arms for use in self defense all but impossible (Murphy, 2009).

2. Pirates or Hostage Takers and Their Indirect Victims

One of the most interesting aspects of Somali piracy is the taking of crews. This is nearly unique to Somalia (Ploch, 2008). This would almost constitute sea kidnapping more than true piracy. This does bode well for those taken by Somali pirates; there have been no wanton displays of violence against those captured. The pirates benefit two-fold from this approach. They benefit in that they are more likely to receive higher ransom for unharmed hostages. The pirates further benefit in that they avoid (with few exceptions) violent confrontation with coalition navies.

The long-term impact of piracy is difficult to measure. In a report to Congress on 4 February 2009, Peter Chalk, a senior representative of the Rand Corporation, estimated that the annual cost of piracy to the maritime industry ranged from one to 16 billion dollars. The maritime underwriters Lloyd's of London have designated the Gulf of Aden a "War risk zone" (Ploch, 2008). This can raise the premium paid by companies from 10 to 20 thousand dollars per trip through the gulf. London-based firms have shown a willingness to pay smaller ransoms on the order of $500,000 up to $2 million USD (Ploch, 2008). Ransoms higher than that are not paid and typically negotiated down. Fortunately this does not hold true for the tiny American Merchant Marine, insurance premiums have not gone up due to the infrequency of attacks on U.S. shipping. Shipping companies must now weigh the risks of piracy against the added cost of changing the shipping route to avoid the threat. While thousands of ships choose to risk pirate attack every year, the Suez Canal authority has noted a decrease in traffic over 2008 which they directly attribute to piracy.

International commerce is not the only victim of Piracy. There are an estimated 5 million Ethiopians dependant on Humanitarian Assistance (Ploch, 2008). The United States spent $600 million on humanitarian aide to Ethiopia in 2008. This presents low hanging fruit for the pirates. Pirates can both ransom the crew as well as move the cargo ashore, feed their pirate towns and sell what they do not consume. The piracy threat, along with an increase in fuel and shipping prices, has hampered efforts to get aide to the region.

3. The Response

The international response to piracy has been varied. The European Union started Operation ATALANTA, as a direct response to the attacks on WFP ships. Forces assigned to ATALANTA are tasked to escort merchant ships and are authorized use of force to deter pirates. This operation is the first under the framework of the European Security and Defense Policy (ESDP) and will involve over twenty ships and 1,800 personnel. Since the start of Operation ATALANTA, the EU has also opened the Maritime Security Center Horn of Africa (MSC-HOA). The MSC-HOA is voluntary

information exchange where ships transiting the area can provide and receive information as well as coordinate with ATALANTA forces in the area (Ploch, 2008).

The United States' response to the modern pirate threat was the creation of Combined Task Force (CTF) 151. CTF 151 is the first force designated for the sole purpose of combating piracy off the Horn of Africa (Ploch, 2008). Prior to the creation of CTF 151, CTF 150 created a Maritime Security Patrol Area (MSPA). This Area created safer shipping routes for merchant vessels attempting to cross the Gulf of Aden. Within the MSPA lies Internationally Recommended Transit Corridors (IRTC), all U.S. shipping has been directed to plan their passages using the IRTCs. IRTCs are credited for the reduction of successful pirate attacks (Ploch, 2008). The IRTCs are not a panacea however. The incident involving the MAERSK *Alabama* is definitive proof both that not every ship instructed to follow the IRTC does so, as well as the implications of ships that do not following them. CTF 151 forces are coordinated through NAVCENT headquartered in Bahrain.

In 2008, NATO has also coordinated a response in the form of Operation Sea Shield. Sea Shield was a coordinated escort system that would last roughly a year. In 2009 Operation Allied Protector was launched. Allied protector is commanded by the Standing NATO Maritime Group (SNMG). Operation Allied Protector's mission was to deter and defend against piracy off the Horn of Africa. In the Second half of 2009 the mission of Allied Protector was expanded to coordinating with local governments for piracy prevention (Ploch, 2008).

The International Maritime Organization (IMO) is an organization overseeing the commercial shipping industry, based out of London the IMO's "main task has been to develop and maintain a comprehensive regulatory framework for shipping and its remit today includes safety, environmental concerns, legal matters, technical co-operation, maritime security and the efficiency of shipping." (International Maritime Bureau, 2010). As stated the IMO is the organization responsible for the reporting of incidents of piracy involving merchant ships. IMO regulation XI-2/6.6 states,

> The Committee noted that SOLAS regulation XI-2/6.6 requires that an Administration receiving notification of a ship security alert shall notify

> the States in the vicinity of which the ship is presently operating. The Committee confirmed that the appropriate recipient for such information is the national point of contact as required by SOLAS regulation XI-2/7.2, as notified to, and promulgated by, the Organization in accordance with SOLAS regulation XI-2/13.1.5. Where the State(s) in the vicinity of the ship are non-Contracting parties to SOLAS, such information should be passed via normal diplomatic channels in the most expedient manner. (International Maritime Bureau, 2010)

While this direction is important in legal terms, the "Administration receiving notification of a ship security alert" has discretion as to whom they report to. Were the "Administration" directed to report to the MOC itself significant time savings could be realized. SSAS is a technology easily enveloped into the current Navy MOC architecture that if implemented may speed up the time it takes for a competent agent to respond to an incident of piracy.

The SSAS box works as a discrete way to notify individuals of a pirate or terrorist act upon a vessel. A box is installed on the ship, usually the bridge area and in the event of an attack an alarm button can be pressed that sends a distress signal, other alarms can be installed in the Engine Operating Space as well as the Master's cabin (Wireless, 2009). The distress signal is usually sent in the form of an e-mail via INMARSAT or Iridium or through SMS messages. SSAS alerts can be delivered through a variety of means. Information is delivered through transmittal of a ship-to-shore security alert via HF radio, satellite, and/or GSM phone to a competent authority designated as by the company i.e., existing DoD and DON network architectures. The system uses the ship's existing communication systems and connects the alert terminals to the Ethernet on the vessel as with any other digital device.

Current architectures closely guard information through a robust private satellite network, while ensuring reliable service around the globe. These satellite network categories are generally divided between the INMARSAT satellite network, and the Iridium satellite network. The Iridium network consists of 66 Low Earth Orbit (LEO) satellites that have the ability to provide global coverage including the North and South Poles. The downside however to the LEO configuration lies in the possible gaps in coverage. LEO satellites provide 8 to 10 minutes of coverage before connection with the

satellite is lost. The INMARSAT network relies on a Geo-synchronous orbit (GEO) offering global coverage while requiring only three satellites regardless of longitude.

E. COMMAND AND CONTROL IN PIRACY

1. Overview

As more merchant shipping is taken by Somali pirates the opportunity arises to study how rapid accurate notification of incidents of piracy can improve the command and control process. As information is the lifeblood of the command and control system it is imperative to report accurately and timely incidents to the appropriate authority such that the responding force is on scene before pirates have had an opportunity to board but at a minimum before crew and vessel have been taken back to pirate havens along the Somali coast. This information is of particular interest to the U.S. Navy which, due to its capabilities and presence, is often called to respond to incidents of piracy. As the Navy's numbered fleets stand up Maritime Operations Centers (MOC), consideration should be given to how information regarding emergent or crises situations at sea is received and processed at the MOCs. Again, using piracy as the example of an emergent situation at sea this research aims to test various organizational structures and reporting procedures of incidents of piracy and explore how those incidents are managed.

2. Pirate Command and Control Structures

Part of being able to dictate the pace and direction of operations is the ability to move quickly and accurately through the steps of the OODA loop directing one's own forces but also by simultaneously working to disrupt the OODA loop of an adversary. The same is true of Somali pirates. The best way of helping to disrupt their OODA loop in the pursuit of merchant vessels is to understand their command and control and command and control system. This helps to identify areas of weakness for exploitation and to gain perspective on areas of how Somali pirates organize forces and control them when executing a mission.

A command and control system (C2 System) consists of, "the facilities, equipment, communications, procedures, and personnel essential to a commander for

planning, directing, and controlling operations of assigned forces pursuant to the missions assigned" (Department of the Navy, 2008). The first element essential to Somali pirates C2 systems are people. Although their organizations are not explicitly known, Somali pirate gangs are formed along clan lines and recruit personnel primarily from three groups. The three groups are ex-fishermen, former militiamen, and technically savvy individuals (Hunter, 2008). Ex-fishermen provide the requisite maritime knowledge to include ship handling and navigation. Ex-militiamen provide the muscle and weapons knowledge required for boarding's and guarding of hostages. Technical experts provide the know-how to operate commercially available technology such as satellite phones, GPS, laptops, and various pieces of military hardware that require technical acumen. These three groups comprise the core of personnel necessary for pirate operations and of the C2 system; however, there are additional personnel essential to operations. This includes finance personnel, negotiators, cooks and care takers for hostages and weapons procurement personnel (Hunter, 2008). Pirate organizations additionally have a ready pool of recruits from young disaffected Somali youth that with little hope for employment will easily turn to piracy to secure a living.

The facilities that pirates require as part of their C2 system are first and foremost the ports from which they operate out of. Ports in Somalia that have been identified as havens for pirate gangs are Eyl, Haradhere, Bosaso, Qandala, Caluula, Bargaal, Hobyo, Mogadishu, and Garad (Ploch, 2008). Within these ports the pirates rely on facilities for shelter, food, and buildings to keep hostages. A key characteristic shared by these port cities that make them advantageous for pirate gangs to be based at is they are strongly armed, have sympathetic populations, and are in areas beyond the control of the local Somali Transitional Federal Government (TFG). The map depicted below shows the ports that have significant pirate activity.

Figure 9. Port towns of Somalia and Puntland. (From Ploch, 2008)

A variety of equipment makes up the Somali pirate C2 system. The main pieces of equipment are the boats and weapons they employ when attempting to board a merchant vessel. Pirates operate 20-foot-long fiberglass hulled skiffs. These skiffs are powered by one or in some cases two outboard motors ranging in horsepower from 85 to 150 horsepower. For operations involving greater range pirates use pirated fishing trawlers or dhows, also named mother ships, which can hold more supplies and personnel than the smaller skiffs. Skiffs are also tied up alongside mother ships (International Expert Group on Piracy off the Coast of Somalia, 2008). This equipment combines to provide the pirates with a versatile platform for operations on the high seas. For boardings of merchant vessels pirates use ladders, grappling hooks and rope as well as GPS navigation systems to fix positions of merchant ships and coordinate assets.

Communications allows for critical information to flow for an organization within the C2 System. The pirates communicate through a variety of means. The pirates use satellite phones to communicate with each other as well as when negotiating ransom demands to organizations trying to pay ransom to the pirates in exchange for hostages (International Expert Group on Piracy off the Coast of Somalia, 2008). Pirates use laptops for business transactions and therefore it is possible they utilize such applications as email and chat to communicate as well. Additionally when conducting an attack on a

merchant vessel with two or more skiffs pirates may use line of sight handheld radios to communicate at the tactical level. In port towns pirates may use messengers delivering oral or written directions. Pirates also use successfully hijacked vessels onboard communications systems to conduct ransom negotiations (International Expert Group on Piracy off the Coast of Somalia, 2008).

The procedures that allow the pirate gang to prosecute merchant shipping for hijacking and ransom are not exactly known. While tactics have been observed on how they board vessels it is unclear as to who gives the orders to attempt a hijacking. Although it is an issue of much debate, "there are also reports of pirates being equipped with GPS and tracking ships through the use of on board navigation information systems. They are also believed to have built up a large network of coastal and port informers who are able to pass on relevant information to them when required" (International Expert Group on Piracy off the Coast of Somalia, 2008). Such procedures help to direct pirates at sea close to a targeted merchant vessel and give pirate group leaders the ability to plan in advance as opposed to early tactics which involved loitering at sea until a suitable target passed by.

The items involved in the Somali Pirate C2 system described individual pieces that make up form two elements of a C2 System. The first element is the personnel and the second element is the facilities, equipment, communications and procedures collectively. These elements are, "…essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned" (CJCS, 1995).

F. WHY HAS THIS PROBLEM NOT BEEN SOLVED?

A look at U.S. response to incidents of piracy throughout history can lead to discoveries of what made for successful intervention or led to disaster on the high seas. In all of the examples highlighted by this research they all received presidential attention to the issue. The presidential attention for each issue also meant that the Office of the President was ultimately responsible for dictating to military forces what action the United States would take. This process running its course all the way to the highest level

of U.S. decision making adds a considerable amount of time to responding to singular acts of piracy. The dissemination of clear concise commander's intent would allow for lower level commander's to position their forces to exploit many of the advantages Decatur benefited from in the early 19th century.

The evolution of communications flow allows for the United States to now respond to singular incidents of piracy. At the time of the *Edwin* incident, which due to much U.S. public outcry led to the deployment of Decatur and his Mediterranean Squadron, communications moved at the speed of sail at sea or by foot or horseback on land. The United States therefore could do little to respond to one incident in piracy but had to deal with the culmination of incidents. The actions of the Decatur's squadron were a response to the pirate threat in Mediterranean waters not the taking of the *Edwin*. As long range radio communications and later satellite communications came into existence the United States was able to be notified of a singular incident quickly. Response could happen quickly depending on the proximity of U.S. forces. This meant that while attempting to deal with many of the socio economic issues on land that allow for piracy to flourish the United States could still affect positive outcomes of individuals taken at sea.

Modern day merchants have an established pattern of paying ransom to pirates similar to the practices of American merchant shipping prior to President Madison dispatching Decatur to the Mediterranean for the second time. The paying of ransoms did not work at this time and is not working in present day Somalia as piracy is becoming more and more established and expanding to an international business. Unlike the early situation in the Mediterranean where there was not a USN presence, today in the Indian Ocean and GOA the USN patrols these waters ready to respond to an incident of piracy. Effective organizational structure and reporting of incidents of piracy between commercial shipping companies and the USN must be critically examined to allow the USN a chance to respond to and plan for incidents of piracy where force is necessary to take back the ship.

The *Achille Lauro* incident and the *Alabama* incident saw the utilization of U.S. special operations forces. These responses while successful can tie up assets that could

be utilized elsewhere in response to other crises. In all of the examples the on-scene commander had clear commander's intent from higher authority, be it the Secretary of the Navy or the President. Additionally, the on-scene commander had permission to use deadly force if needed as was the case with the Maersk *Alabama* situation. The focus of these efforts to this point has been on the physical response to piracy. This thesis hopes to shed some light on possible improvements in the reporting process to bring about a quicker response by the U.S. government and coalition partners.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

A. WHY POW-ER

POW-ER is a well established computational model in the academic field with its development at Stanford as a part of the collaborative Virtual Design Team. The Office of the Assistant Secretary of Defense for Networks and Information Integration has sponsored initiatives regarding POW-ER. POW-ER was chosen for this thesis to model reporting, coordination, planning and decision to allocate forces for an incident of piracy. Current methods are modeled in the "As Is" scenario. The proposed benefits of the SSAS model can be seen in the results of the experiment using the "To Be" scenario. POW-ER modeling software has been accepted in the academic community having been developed at Stanford and utilized heavily at the Naval Postgraduate School to model edge organizations as well as various commercial entities. POW-ER is a concise way to gain qualitative data to help solve decision making problems about the structure of an organization.

1. History of POW-ER

The Virtual Design Team (VDT) research group was initiated at Stanford in the late 1980s to, "…help managers design organizations and work processes for executing fast-track development of complex products without incurring the large cost overruns and catastrophic quality failures that had frequently plagued such efforts" (Leavitt, 1965). The VDT simulation system is a computational model of project organizations, the first commercial implementation of the VDT software was introduced in 1996 known as SimVision (Leavitt R. E., 2009). VDT has limitations in trying to model edge organizations and requires models to have, "…a defined beginning and end, predefined sequences of tasks with estimable amounts of direct work, and predetermined actor task assignments" (Leavitt, 1965). Despite these limitations the success of SimVision led to four later versions of VDT software, the fifth version known as VDT-5 was released as POW-ER 3.3 to the U.S. Navy.

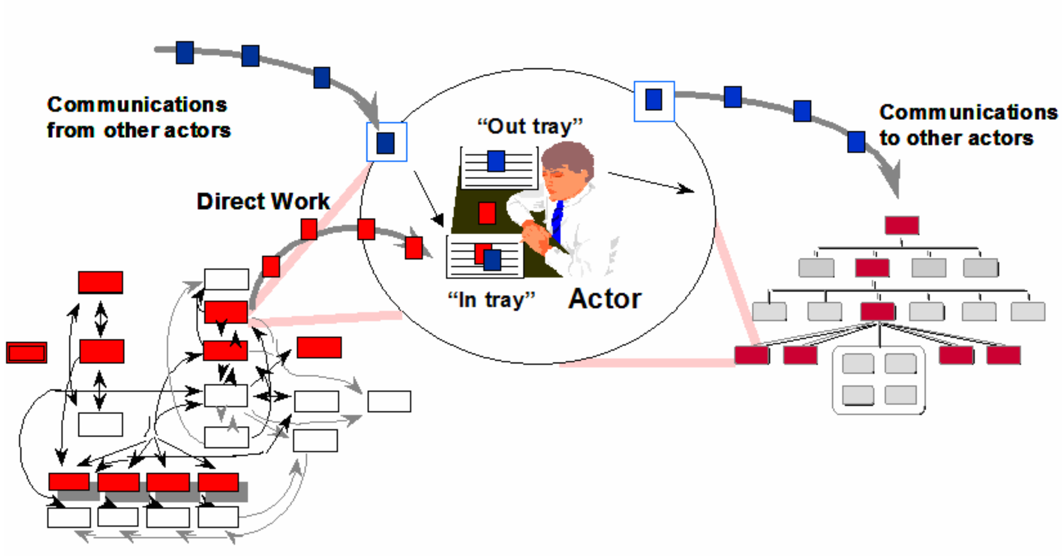

Figure 10. VDT Processing View of Knowledge Work (From Levitt, 1965).

Due to these limitations POW-ER 2.0 was developed so behaviors such as knowledge flows, trust effects and cultural differences between team members within highly distributed organizations could be modeled in a research environment. Additionally POW-ER can model, "…demand-driven, dynamic allocation of resources to tasks on an as-needed basis" (Leavitt, 1965).

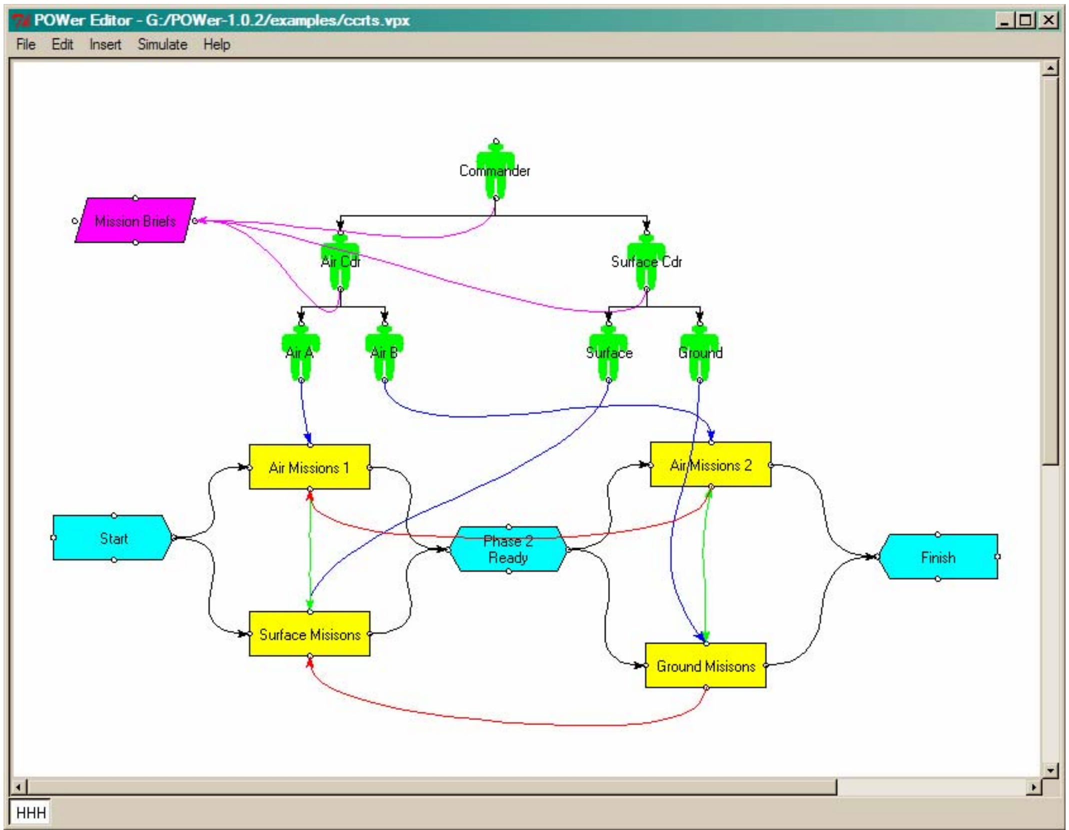

Figure 11. Sample POW-ER model (From Levitt, 1965)

The above screen capture shows the graphical user interface for POWER in this case the model represents a simple Command and Control (C2) structure. In the model actors, tasks, milestones, meetings, communication links and their relationships are represented. POWER is capable of modeling tasks ranging in time from minutes to years. The POWER platform is made up of a graphical model editor, simulation engine, and a charting and reporting module. "The model editor provides the primary user interface to POW-ER. It allows for the construction of complex project models by dragging, dropping and connecting simple graphical objects representing actors, tasks, meetings, etc., along with the relationships between these objects. A property editor supports direct manipulation of the numeric and symbolic properties specific to each type of object. The model editor also supports automatic derivation of alternate versions of a model, supporting comparative analysis of related scenarios" (Leavitt, 1965). In order to

simulate the model POWER uses Monte Carlo techniques, the use of these techniques allows for a model of complex systems involving large numbers of actors.

2. Academic Justification

Extensive testing has gone into POW-ER as a successor to VDT at the academic level. As Dr. Raymond Levitt of Stanford University comments, POW-ER is going to be heavily utilized to model organizational structures. With an ultimate goal of being able to, "…supply a robust organization design and planning tool that can be used by the wider C2 community to engage in sophisticated "what-if" analysis of real world situations" (Levitt, 1965).

A thesis from June 2008, utilized POW-ER software to model Extended Maritime Interdiction Operations (MIO) organization, data collection and information flow. The Sundland Carroll thesis used POW-ER to model the current organizational structure for the way EMIO is conducted and then modeled a proposed organizational structure for EMIO operations designed to decrease the time to conduct the mission and process information (Sundland, 2008).

In 2006, this paper, "Computational Modeling and Analysis of Networked Organizational Planning in a Coalition Maritime Strike Environment" at the 2006 Command and Control Research and Technology Symposium: The State of the Art and the State of the Practice. This research begins with documenting the planning process associated with maritime tasking orders for a coalition expeditionary strike group. The research is then used to build a model of the current maritime component commander organization and planning process using the POW-ER software. Alternatives to this are explored and measured through the quantitative data generated by POW-ER (Looney, 2006).

POW-ER has been discussed as being a cost effective way of gathering data on hypothesis before conducting costly and time consuming field experimentation. "Clearly computational experimentation using tools such as POW-ER (e.g., Gateau et al. 2007) will continue to play a key role in research along these lines. It is very time-consuming

and expensive to grow an Edge organization in the field, but it is very quick and cheap to model and simulate one via computer" (Barrett & Nissen, 2008).

In looking to improve Navy response times to incidents of piracy through optimizing command and control relationships and information flows, POW-ER is capable of modeling the current organizational structure in place to respond to an incident of piracy. The response to piracy involves coordination between the USN and a commercial entity in attempting to conduct a real world exercise involving these two organizations it may be difficult to bring both organizations together. POW-ER is capable of bridging this gap and modeling the interaction between these two entities. Since POW-ER is capable of large numbers of replications statistical relevance is achieved yielding richer quantitative data.

POW-ER allows replications for multiple C2 structures and compares the results side by side. Attempting to do this through real life experimentation could be prohibitively expensive and time consuming for an organization if it were to participate in several different types of experiments aimed at modeling their command and control structure. Research involving POW-ER has been sponsored by the Office of the Assistant Secretary of Defense for and Information Integration. The research was for the Command and Control Research Program (CCRP).   The Navy has recognized the efficacy of using POW-ER to model existing and hypothetical C2 structures with specific examples of POW-ER being used to study command and control possibilities pertaining to the MOC. As this thesis looks at part of the Navy MOC, it is valid to use POW-ER software to gather quantitative data to analyze the time it takes for the Navy to respond to an incident of piracy.

B. IDENTIFYING POW-ER EXPERIMENT CONSTANT PROPERTIES

1. Overview

Many properties will remain constant through all experiments modeling the MOC anti-piracy operations, these constants are described through their properties and are broken down between Project, Case, and Position properties. For the models generated using POW-ER the term "Property" or "Properties" is used in the place of "Attribute."

Likewise, the term “Position” is used in place of the term “Actor.” Position properties will not change between experiments to simulate the same people conducting varied tasks as the MOC architecture changes.

The term “Project” refers to the model as a whole, while a “Case” is a specific configuration within a model. In this case both the “As Is” and “To Be” are two cases of the same project. Project and Case properties are those that apply to the whole architecture and will remain constant through all the experiments.

2. Project Properties

These properties are universal between cases and did not differ between experiments. The priority for this experiment is high due to the level of attention given to individual acts of piracy. The work day is set to 1440 minutes to reflect the 24 hour workday of the MOC, likewise the workweek is set to 10,080 minutes to reflect the seven day workweek of the MOC. The team work experience is set to medium to allow for differences in ability between watch-standers. Centralization of the MOC organization is set to low to show to reflect the individual efforts of the watch-stander. Each watch-stander’s contributions stand on their own and though the Course Of Action decision requires higher approval individual tasks assigned can be completed by the persons assigned. Formalization for the experiment is set to high to reflect the structure of Pre-Planned Responses, Rules Of Engagement and standing orders within the theater. The Communication Probability is set to 00.85 to allow for gaps in communication due to watch turnovers and human error. The Noise probability is set to 00.01 assuming there is a 1% chance of noise cancelling out communication. Functional Exception Probability is set to 00.01 because of an assumed very low probability that the tasks assigned would be beyond the capabilities of those assigned to the task. The Project Exception Probability and the Institution Exception Probability are set to 00.01 assuming a very low probability of interface problems between tasks.

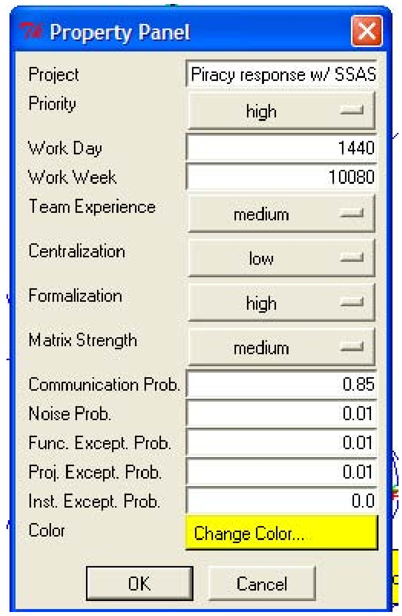

Figure 12. Project Properties for all MOC experiments

3. Case Properties

The case properties will not change between the cases as the name would imply. Keeping these values constant demonstrates their role as independent variables in the experiment. The start date for both cases is 01 April 2010. The seed value is 0 to run a truly random simulation for 10,000 trials. The Actor-Model is set to Generic and Skill-Model is set to Static so they will not bias the results of the experiment.

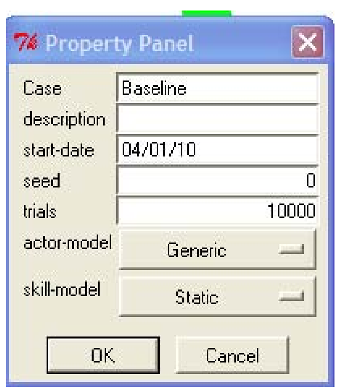

Figure 13. Case Properties for all MOC experiments

4. Position Properties

These properties will be described by role but will be constants through all the experiments. The Culture of the position can be defined as Generic, Japanese or American, for this series of experiments the culture will be set to American for all positions. The role of the Position can be defined as a Project Manager (PM) the highest level decision maker, a Subteam Lead (SL) the decision maker subordinate only to the PM, or a Subteam Member (ST) who is merely a worker. The Full Time Equivalent (FTE) is the amount (represented by percent) of attention a task is given by a position. The Application Experience describes the experience of the person(s) filling a position. Cultural Experience marries the culture of the person in the position with the organization's design, for all runs the Cultural Experience will be set to medium. Salary is not a motivator for the positions and is set at the default 50.0 for all runs. The skill ratings will remain at their default settings with no setting changes.

To explain the statistical probability of supervisory agents becoming involved in direct support of tasks not completed, consider two independent tasks, Task A and Task B. A supervisor must take remedial action if one or both tasks fail. So, what is the probability that Task A fails OR task B? It is the complement of the probability that Task A AND Task B are successful.

P(Task A fails) = 0.01
P (Task A succeeds) = 1- 0.01 = 0.99

P(B fails) = 0.01
P(B succeeds) = 0.99

P(A AND B succeeds) = P(A success) * P (B success) = (0.99)^2
Thus, P(A or B fails) = 1 – P(A AND B succeeds) = 1 – (0.99)^2

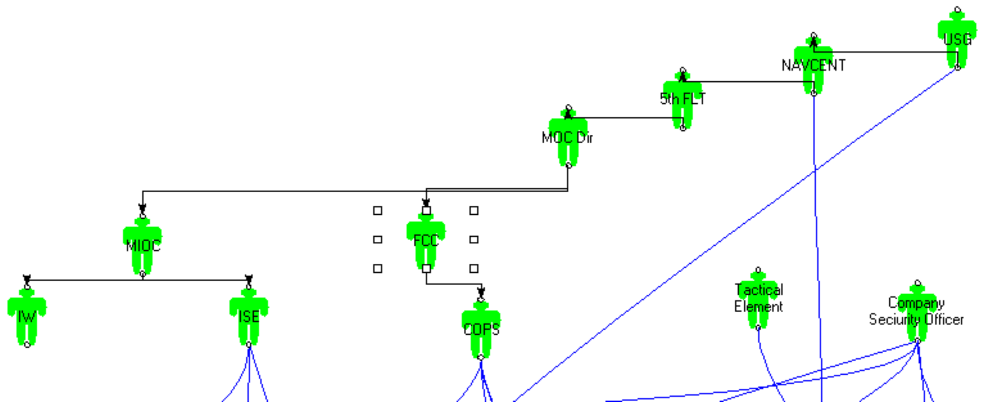

Figure 14. MOC position Construct

a. U.S. Government

The position titled U.S. government is not meant to represent one individual person but the collective efforts of all those involved in responding to an act of piracy above the level of NAVCENT. The role for this position is set as PM. The Application Experience is set to medium to allow for the “quality spread” among all the persons involved. The FTE for the U.S. government has been set to 00.6 to reflect the attention given by a hegemonic government that cannot focus all its efforts on one task. Given the number of tiers between the U.S.G position and the IW/ISE/COPS positions and the Functional Exception Probability of 00.01, there is a 0.01x 2.989^{-7} (2.989^{-7} is based on the probability of failure by lower-level position to complete a task) or 2.989^{-9} chance that the USG position would have to directly solve any tasks not handled by any of the lower level positions given a Functional Exception Probability of 0.01. The Functional Exception Probability can be manipulated (set higher or lower) within the model to emulate the decision making characteristics/personality of a specific USG element/leader.

b. NAVCENT

The NAVCENT role represents both the decision maker and his staff. The position is given the Role of SL with NAVCENT being the decision maker subordinate to the USG but responsible for the Course of Action decision. The Application Experience is set to medium due to the counter-piracy planning and action being one of many

warfare areas for which NAVCENT is responsible. The FTE is set to 00.8 due to the priority of planning contingencies to the piracy scenario among the staff while not losing the commander's focus on the remainder of the theater. The Functional Exception Probability for this experiment leaves the NAVCENT commander and staff with a (0.01 x 0.00002989) or 2.989^{-7} chance of having to directly solve a task assigned to either the MIOC or the FCC.

c. 5th FLT

The 5th Fleet position represents the 5th Fleet commander and staff. This position is given the role of Subteam member to account for the 5th Fleet's responsibility for the MOC while being responsible to NAVCENT. The Application Experience is set to medium. The FTE for 5th Fleet has been set to .80 to reflect the level of attention required by the numbered fleet commander. The 5th Fleet position has a (0.01 x 0.002989) or 0.00002989 chance of directly solving a task assigned to MOC positions based on a 0.01 chance of the 0.002989 chance lower echelon failure.

d. MOC Director

The MOC director represents the person assigned as the MOC director. The MOC director's role is that of a Subteam Lead for the responsibility of those in the MOC. The Application Experience is set to medium as there is no requirement for previous anti piracy experience when screened. The FTE is set to .8 to show the attention given by the MOC Director to an incident with U.S. civilian mariners as hostages, using the join statistics method the MOC director has a $[1-(1-.0199 \times 0.01)(1-.01^2)]$ or 0.002989 chance of becoming directly responsible for incomplete tasks performed by their subordinates.

e. Maritime Intelligence Operations Center (MIOC)

The MIOC position serves as the person heading the Intelligence cell within the MOC. This person is designated as a Subteam lead responsible for the Indications & Warnings position and the Intelligence Support Element position. The Application Experience is set to medium and the FTE is set to 00.65 due to the high level

of intelligence data and information passing through the 5th Fleet area of operation not pertaining to piracy. There is a ($1\text{-}0.99^2$) or 0.0199 chance that the MIOC position will have to complete a task assigned to the I/W or the ISE.

f. Fleet Command Center (FCC)

The FCC position represents the person assigned to run the Operations cell within the MOC. The role is set to Subteam Lead responsible for the Current Operations position. The FTE for the FCC position is set to 00.70 because of the Operations other than piracy that must be actively coordinated in the region. The Fleet Command Center hold the same supervisory position as the MIOC, however due to the nature of the response planning for individual incidents of piracy the Current Operations (COPS) is the only position tasked beneath the FCC. Given this, the FCC has a 0.01^2 or 1^{-4} chance of having to directly complete tasks assigned to COPS.

g. Indications and Warnings (IW)

The IW position represents the cell responsible for receipt, processing, initial analysis of and rapid dissemination of time-sensitive intelligence within the MIOC (Department of the Navy, 2008). IW is also responsible for monitoring red and white shipping. The role assigned to the IW position is Subteam member. The FTE for this role is 0.90 due to the IW's responsibility of initial analysis of the pirate attack. The Functional Exception Probability of the IW position is set to 0.01 given the formal and on-the-job training prior to a watch-standers qualification, in other words there is a 1% chance the IW position would not be able to complete an assigned task.

h. Intelligence Support Element (ISE)

The ISE position represents the cell within the MIOC responsible for the Intelligence Preparation of the Operational Environment (IPOE), Knowledge and Information Management (KIM), support for the commander's assessment and IO (Department of the Navy, 2008). ISE is assigned the role of Subteam member and is given an FTE of 0.65, ISE is given an FTE of 0.65 because it will continue to have other intelligence requirements throughout the region to various customers in the MOC and

therefore will not devote all available resources and time to an incident of piracy. ISE also has a Functional Exception Probability of 0.01 due to the knowledge base within the cell.

i. Current Operations (COPS)

The COPS position represents the planning cell within the FCC responsible for ongoing and emergent operations. The FTE is set to 0.85, assuming the planning of a response to an emergent act of piracy would consume 85% of the cell's efforts. The Functional Exception Probability results in a 1% chance the COPS team would not be able to complete an assigned task.

j. Tactical Element

The Tactical Element position represents a wide array of elements within the military from tier one Assets (e.g., Development Group) to a special operations capable Marine Expeditionary Unit. The role of the Tactical Element is given the role of Subteam Leader. The FTE for this position is 1.0 because when tasked all the efforts of that specific element are focused on the anti piracy mission. There is a 0.01 Functional Exception Probability for this position.

k. Company Security Officer (CSO)

The CSO position represents the shipping company that owns the victim ship down to the person within the company (CSO) that coordinates between that ship and the USG. The culture of the interactions between the company and the USG will be defined as American for the role assignment. The settings for organizational culture in POWER are American, Japanese or Generic. Shipping companies are headquartered all over the world however to function in this organizational model the interface is inherently American. The FTE of the CSO is set to 0.9 given the priority of managing ransom demands, employees held hostage and potentially lost cargo.

C. IDENTIFYING POW-ER EXPERIMENT VARIABLE PROPERTIES

1. Overview

The POW-ER Modeling software allows for the control of many variables. These variables will change to reflect changes to the overall architecture being modeled. These variables will be identified as Task, Assignment and Branch properties. Task properties will change as the design of the MOC changes to incorporate new technologies (SSAS). Assignment properties will change with the changing tasks. Branch properties will change to accommodate the time required to move from task to task as the MOC architecture changes to include SSAS.

Experiment 1 for this thesis focused on the current command and control architecture for 5th Fleet Maritime Operations responding to an emergent act of piracy committed against a U.S. flagged merchant vessel. Responsibility for the reporting of this incident to the U.S. government (USG) falls on the commercial shipping interest represented by the company's security officer. This model hopes to emulate the sequence of events that occurred during the Maersk *Alabama* incident.

2. Experiment Milestones

Milestones in POW-ER are used to detail phases of completion for the work flow. The milestones for the experiment follow the phases of the commander's decision cycle as delineated in the MOC Concept of Operations (CONOPS) NTTP 3-32.1. Those milestones include "Monitor," "Assess," "Plan" and "Direct." "Monitor" marks the start of the experiment and includes all MOC operations prior to the incident of piracy. The "Direct" milestone ends the experiment with the commander's decision communicated. Events after the commander's decision including logistical positioning and actions taken to physically counter the act of piracy securing the M/V ship and crew are not included in the model. Definitions of the Milestones taken from NTTP 3-32.1 are included below.

a. Monitor

Monitoring involves measuring ongoing activities that may impact the operational area or impact ongoing or future operations. The baseline for this

measurement of the situation is the current plan or plans. This baseline allows the staff to measure the current situation against the one envisioned in the plan. This allows the commander and staff to identify where the current situation deviates from the one envisioned in the plan. Although staff sections monitor their individual staff functions to maintain current staff estimates, the preponderance of monitoring is conducted by the maritime intelligence operations center (MIOC), the Navy operations center, the logistics readiness center (LRC), and the communications and information center (Department of the Navy, 2008).

b. Assess

Within the commander's decision cycle, assessment is the determination of the impact of events as they relate to overall mission accomplishment. Fundamental to assessment are judgments about progress in designated mission areas as measured against the expected progress in those same mission areas. These judgments allow the commander and the staff to determine where adjustments must be made to operations and serve as a catalyst for planning. Ultimately, assessment allows the commander and staff to keep pace with a constantly evolving situation while staying focused on mission accomplishment. The maritime assessment group has formal responsibility for assessment, but all MOC organizational entities bear some level of responsibility to be alert to indications that things are not going according to plan and take appropriate action (Department of the Navy, 2008).

c. Plan

In the planning portion of the commander's decision cycle, the commander and staff make adjustments to the current plan or develop new plans with the purpose of successful completion of the broader mission. The preponderance of the planning function is conducted in either in future operations (FOPS) or the maritime planning group (MPG) (Department of the Navy, 2008).

d. Direct

The commander, through the MOC, directs actions to ensure that current orders and directives are completed as intended. This direction is done with the broader purpose of achieving the overall mission. Tools like the commander's intent and commander's critical information requirements (CCIRs) assist the MOC in this role. The preponderance of the directing function is conducted by Navy operations center and current operations (Department of the Navy, 2008).

3. Experiment 1 Tasks

For the purposes of POWER a task is defined by its properties. The first property is the task name and the effort which is the duration of the task given a specified level of required skill. Effort type for a task is the FTE. Each task requires a required skill which will be left as the default setting of generic for this experiment. This required skill reflects the ability of the average worker. The learning days is set to zero implying there are no days required to learn the work, the assumption that everyone is qualified to have their job. Each task has a priority which dictates which task takes precedence for actors that are assigned more than one task. Task properties including "Requirement Complexity," "Solution Complexity" and "Uncertainty are set to the default of Medium for the purposes of both experiments. There is a "Fixed Cost" property of Zero, because financial considerations especially minimizing cost are not the concerns of the workers in the model. This functionality is meant for private industry looking to minimize costs. The associated successor branches will be discussed with the task it affects. The priority property of a task will not affect other tasks assigned to a position because tasks assigned are completed in series. These tasks will start after the "Monitor" milestone and is not concerned with current regional operations within the MOC outside the scope of piracy. These tasks will end when the "Direct" milestone is achieved the physical counter piracy phase of the operation to include logistics positioning and support is beyond the scope of this model.

a. Attack Notification

The name of this task is “Attack Notification.” “Attack Notification” is the first task in the “Monitor” phase of the decision making cycle. This task starts after a given 10 hour time lag between the start of the pirate attack and the shipping company’s notification. This 10 hour time lag accounts for an average of two possible means of attack notification to the shipping company. The first being the merchant vessel notifies the shipping company at the start of the attack marked by visual sighting of pirates following the ship. An example of this is the case of the Maersk *Alabama* where the first sighting of the pirate vessels was the evening before a mid morning attack the next day. The case where a merchant vessel is surprised by a pirate attack and is therefore unable to notify the shipping company that the attack is occurring it would be the pirates who notify the shipping company with a list of demands. The “Duration” of the “Attack Notification” is set to ten minutes accounting for the approximate length of the first communication with the shipping company. The “Priority” of this task is high. This task is complete when the Company’s Security Officer (CSO) receives notification of the attack.

b. Attack Verification

The name of this task is “Attack Verification.” This task is preceded by a 1 hour time lag which accounts for an average time between the CSO being notified in the middle of the night away from work and during the day at work with all available resources to notify pertinent decision makers in the company. The “Duration” of this task is given a time of 1 hour to reflect an easily identifiable false alarm/confirmation of attack or instances where contact cannot be readily established/report of a false alarm is made under duress. The “Priority” of this task is set to “High.” This task is complete when the attack is verified.

c. U.S. Government Notification

The name of this task is “U.S. Government Notification.” This task is preceded by a set 3 hour time lag. This time lag accounts for the time it would take for the shipping company to gather pertinent details regarding the attack to include ship type

and crew on board a best estimate of number of pirates on board and their demands. The "Duration" of this task is set 30 minutes which accounts the first contact with the U.S. government to relay information regarding the attack. The "Priority" of this task is set to "High." The task is complete when the first representative in the U.S. government has been notified of the attack. Following initial USG notification there is an assumed 8 hour time lag which accounts for dissemination of news of the attack to responsible elements within the USG.

d. Corporate Input to the USG

The name of this task is "Corp input to USG." The duration of this task is set to 1 day. This duration allows for the initial decision making process on behalf of the corporation on whether or not USG intervention is desired. The "Priority" of the "Corp input to USG" is set as "High." The task is complete for the purposes of this model when the company decides it would like USG intervention. This marks the end of the "Monitor" phase of the MOC decision making process and begins the "Assess" phase of the MOC decision making process.

e. Mission Analysis

The name of this task is "Mission Analysis." This task is preceded by a 10 minute time lag. This lag accounts for the time the USG representative dealing with the company passes the information to MOC planners to begin planning for a military solution to the incident of piracy. The "Duration" of the "Mission Analysis" task is set to 5 hours and accounts for the time it would take to begin initial deliberate planning and identifying the anomalies surrounding the reported incident of piracy. The "Priority" for this task is set to "Medium" because this task is being looked at by ISE which has other concurrent responsibilities within the MOC. Those other tasks are not reflected in the model. This task is complete when the unique aspects of the incident are identified and "Mission Coordination" is set to begin.

f. “Mission Coordination”

The name of this task is “Mission Coordination.” “Mission Coordination” is the initial assessment of where U.S. forces are operating in the region and liaison with additional forces identified in the “Mission Analysis” task that may be required for the operation. The “Duration” of the task is set to 5 hours and accounts for the time to coordinate with regional forces as well as forces outside of the Area of Responsibility (AOR). The “Priority” of the “Mission Coordination” task is set to Medium to reflect that forces desired may not be available and coordination is based on time management by COPS and the busy nature of a watch floor environment. This task is complete when appropriate forces have been identified for an operation responding to an incident of piracy.

g. Enemy Course of Action Development

The name of this task is “ECOA Development.” The “Duration” of this task is set to 2 hours. This task follows mission coordination to identify significant adversary capabilities and critical operational environment factors. This includes analyzing enemy objectives, Centers of Gravity (COG). Part of this process includes developing enemy most dangerous and most likely COAs. This task is complete when the product supports Blue COA development. The “Priority” of the task is set to “Medium.”

h. Warning Order

The name of this task is “Warning Order.” This task begins, “Once the commander approves the mission following the Mission Analysis briefing and evaluates the factors affecting mission accomplishment…It serves as a preliminary notice of a forthcoming military action with an understanding that more information will follow after the COA is selected” (JMO Deparment, Naval War College, 2008). The “Duration” for the “Warning Order” task is set to 6 hours. This accounts for generating a mission analysis briefing in an hour, an hour to give the brief, and three hours for the commander to decide upon the content of the warning order based upon the briefing presented to him. One hour to generate and disseminate the actual Warning Order message. The “Priority”

of the message is high based on the priority of the end product. The task is complete when the "Warning Order" has been issued. This marks the end of the "Assess" phase of the decision making process and marks the beginning of the Plan phase of the decision making process.

i. Course of Action Development

The name of this task is "COA Development." "COA development planning should consider all joint force capabilities and focus on contributing to the defeat/neutralization of the enemy's Center of Gravity and the protection of the friendly COG" (JMO Deparment, Naval War College, 2008). The "Duration" of COA Development is set to 3 hours to account for the development of three COAs each taking an hour to develop. The "Priority" for COA development is set to high given the fact that given the time sensitive nature of this tasking all work will be devoted to developing each COA. This task is complete when three different COAs have been developed.

j. Course of Action Coordination

The name of this task is "COA Coordination." COA Coordination is marked by analysis of friendly COAs which is a vital step to War Gaming. COA Coordination also compares Friendly COAs against the various ECOAs. The "Duration" of this task is set to 4 hours. Priority for this task is "High" because this is an essential step to the "War Gaming" process. This task is complete when Blue Force COAs are ready to be war gamed.

k. Enemy Course of Action Refinement

The name of this task is "ECOA Refine." This task adds granularity to the initial ECOAs tailoring them to counter the three possible blue COAs. The "Duration" for this process is set to 2 hours. The "Priority" is set to high. The "ECOA Refine" task is complete when the ECOAs have been war gamed against Blue COAs.

l. Course of Action Check

The name of this task is “COA Check.” This task allows the commander and staff to “…develop and evaluate a list of important governing factors, consider each COA’s advantages and disadvantages identify actions to overcome disadvantages, make final tests for feasibility and acceptability and weigh the relative merits of each” (JMO Deparment, Naval War College, 2008). The “Duration” of this task is set to 2 hours to account for overcoming identified disadvantages and a final check to ensure that the COA is achievable. The “Priority” is set to “High.” This task is complete when the Blue COAs are ready to be presented to the decision maker for selection.

m. Course of Action Decision

The name of this task is COA Decision. This task comes after evaluating all the presented COAs. “The staff identifies its preferred COA and makes a recommendation. The staff then briefs the commander…After the decision briefing; the commander selects the COA that most effectively accomplishes the mission” (JMO Deparment, Naval War College, 2008). For the purposes of this experiment the commander is the 5th Fleet Commander. The “Duration” of this task is set to 1 hour. In this time the commander can deliberate on the presented COAs, ask questions and make refinements to a final COA. The “Priority” is set to “High.” This task is complete when the commander has decided upon one COA to accomplish the mission.

n. Action Rehearsal

The name of this task is called “Action Rehearsal.” This is the tactical operator’s chance to conduct a physical walk through of the sequence of events to counter the act of piracy. The duration of this task is set to 4 hours. The learning time for this task is set to 1 day which allows for the action unit to learn the specifics of the mission and the duration of four hours accounts for rehearsal and briefing of the mission. The “Priority” is set to High. This task is complete when the action unit is ready to execute the mission.

o. Corporation's Final Consent for Government Intervention

The name of this task is "Corporate Go/No Go." This task is the shipping company's final decision to allow for military action aboard their ship. They will make this decision after being briefed by the military on the previously decided upon COA. The "Duration" of this task is set to 1 hour. The "Priority" is set to High. This task is complete when the Company gives the authorization for military intervention on its behalf to recover the vessel and crew. This is the last task in the "Plan Phase" of the decision cycle. This is followed by the "Direct" milestone which signifies the completion of the decision making cycle but does not include the actual physical operation to retake the vessel. The below screen capture of the POWER software shows the setup of Experiment 1.

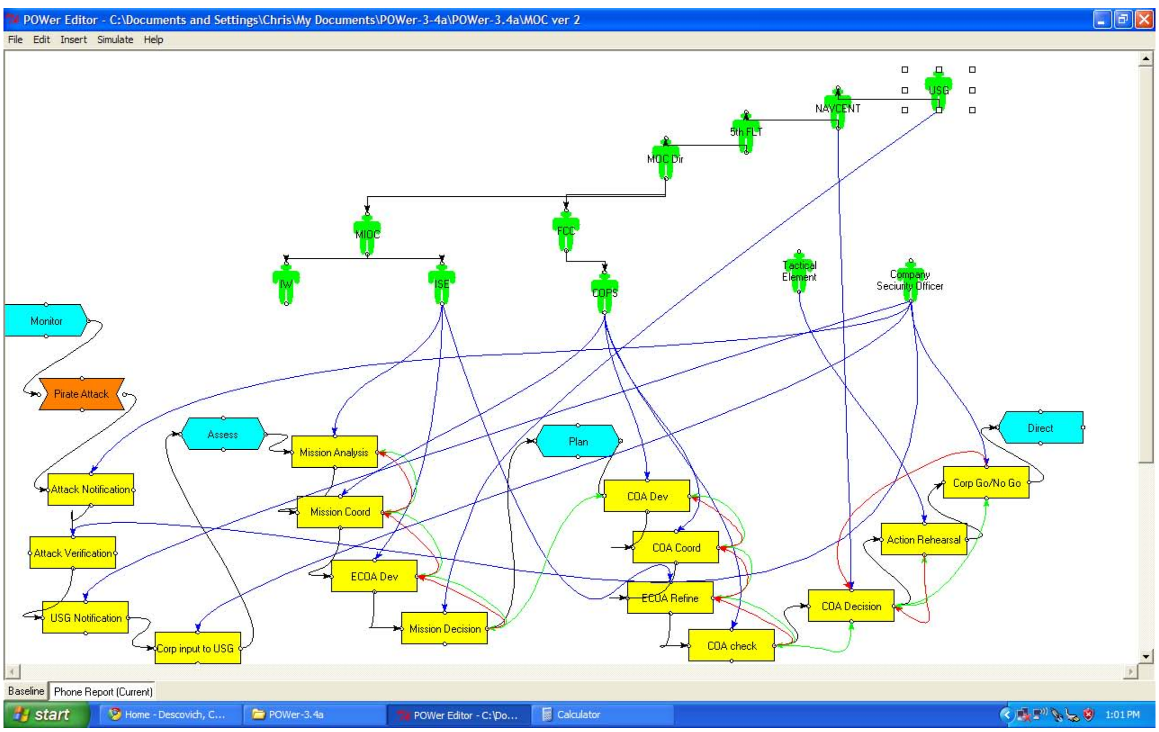

Figure 15. Screen Capture of "As Is" configuration

4. Experiment 2 Tasks

Experiment 2 looks to examine a change in the notification procedures and the input of the SSAS technology into the organizational structure. The "Learning Days,"

"Required Skill," "Requirement Complexity," "Solution Complexity," "Uncertainty," "Effort Type" and "Fixed Cost" properties will be the same settings as they were in Experiment 1. The "Milestones" which make up the decision making cycle of "Monitor," "Assess," "Plan" and "Direct" will remain the same. The property settings of tasks associated with the "Assess" and "Plan" phases will remain the same as Experiment 1, helping to ensure experiment control. The positions within the organization remain the same except for the Company Security Officer is no longer responsible for notification of the attack to the USG. The first task is preceded by the SSAS inject transmitted directly from the merchant vessel being attacked to the I&W cell within the MOC. The SSAS Inject is represented in POWER Model as an "Event." The duration of the "SSAS Inject" is set to 1 minute. 1 minute accounts for satellite relay delay and the human in the I&W cell seeing the inject.

a. SSAS Verification

The name of this task is "SSAS Verif." This is preceded by a time lag of 2 minutes to allow time for the watch stander to start the process of verification. SSAS verification would be conducted by calling the ship itself or calling the company to see if they have received the same information or looking for a near immediate cancellation of the that alarm showing that it was erroneously activated. The "Duration" of this task is set to 10 minutes. If the incident cannot be identified as a system malfunction or activated in error within 10 minutes, the I&W cell will proceed with the information and treat it as an actual incident of piracy. The "Priority" of this task is High given the time sensitive nature of the indication. This task is complete when the I&W watch stander reports the incident to the MIOC Commander as well as COPS.

b. SSAS Report

The name of this task is "SSAS Report." This task represents the time I&W takes to report the incident of piracy to the MIOC commander and COPS. The "Duration" of this task is set to 10 minutes. The duration is set to 10 minutes due to the variety of ways communication of the incident occurs within the MOC. Notification could be through voice communications, chat, and face to face meetings. 10 minutes

represents an average time any of these methods would take to include clearing up any questions that arise from those notified of the incident. The "Priority" is set to high. This task is complete when other members of the MOC outside of the I&W cell are aware of the incident. The below screen capture of the POWER software shows the setup of Experiment 2.

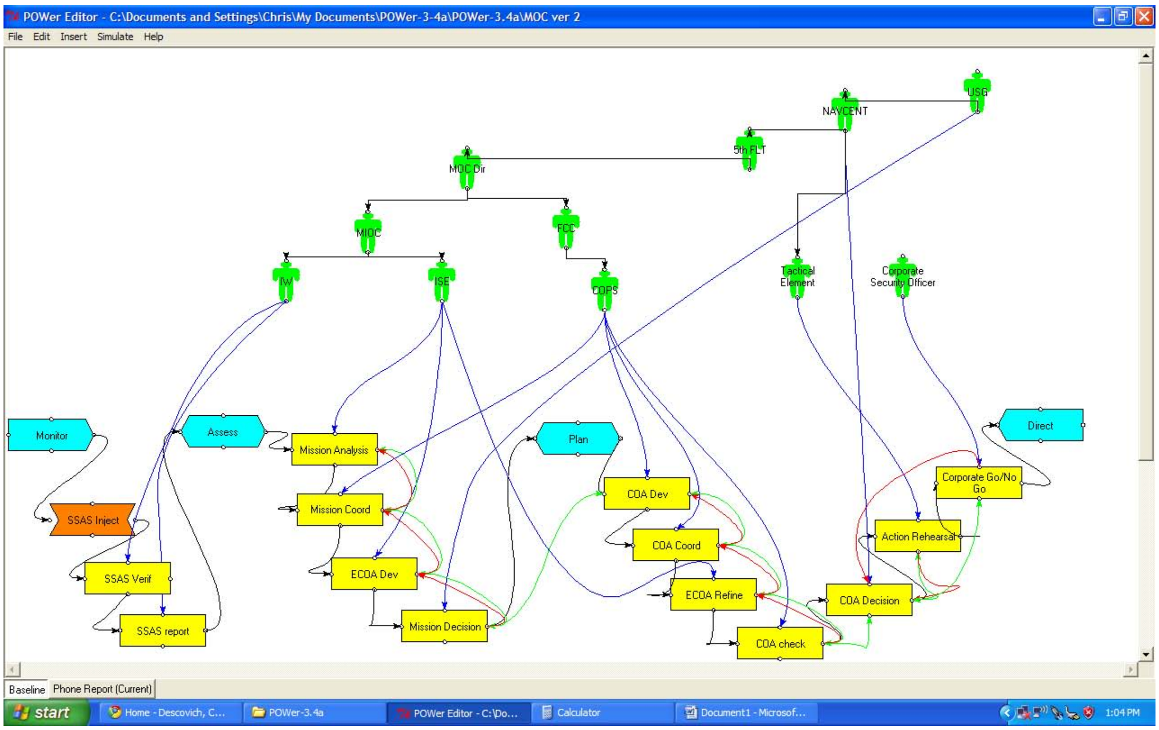

Figure 16. Screen Capture of "To Be" configuration

5. Methods for Interpreting Results for the Experiments

The purpose of modeling these experiments is to capture quantitative data in order to facilitate numerical comparisons, measurable objectives and conduct mathematical analysis of data obtained. Experiment 1 and Experiment 2 will be compared against each other to determine if a decreased variability in timeline to incidents of piracy can be achieved. POWER will simulate each experiment 10,000 times. Simulation is useful because studying responses to piracy is a large complex system with several interaction and interdependencies. A mathematical model that gives empirical data is a more conclusive way to measure the effect of changes to an existing system than qualitative

means. There are limitations to the use of simulations. Simulations are not predictive given the results of the model. Simulations cannot be run only once to arrive at an answer. The model we built for this experiment is case specific and cannot be applied to other warfare areas.

The goal of these experiments is to show a decrease in the variability in the time line of reporting and responding to an incident of piracy. The removal of the shipping company security officer and shipping company deliberating on whether or not to seek USG intervention and the inject of automated reporting via SSAS can aid in intercepting the captured vessel as it steams to pirate safe havens on the coast of Somalia. The automated SSAS report can provide confidence through speed and accuracy of reporting such that ROE can be delegated down to theater decision makers instead of requiring presidential approval.

IV. ANALYSIS

A. DATA COLLECTION

The "As Is" scenario for this thesis focused on the current command and control architecture for 5th Fleet Maritime Operations responding to an emergent act of piracy committed against a U.S. flagged merchant vessel. The "To Be" scenario examined a change in the notification procedures and the input of the SSAS technology into the organizational structure. Time becomes the critical factor in maritime operations planning when considering the distance needed to travel between prepositioned forces and forces dispatched to respond to an incident of piracy. Analysis of the experiments conducted will help optimize positioning of these forces to counter future pirate threats.

1. "As Is"

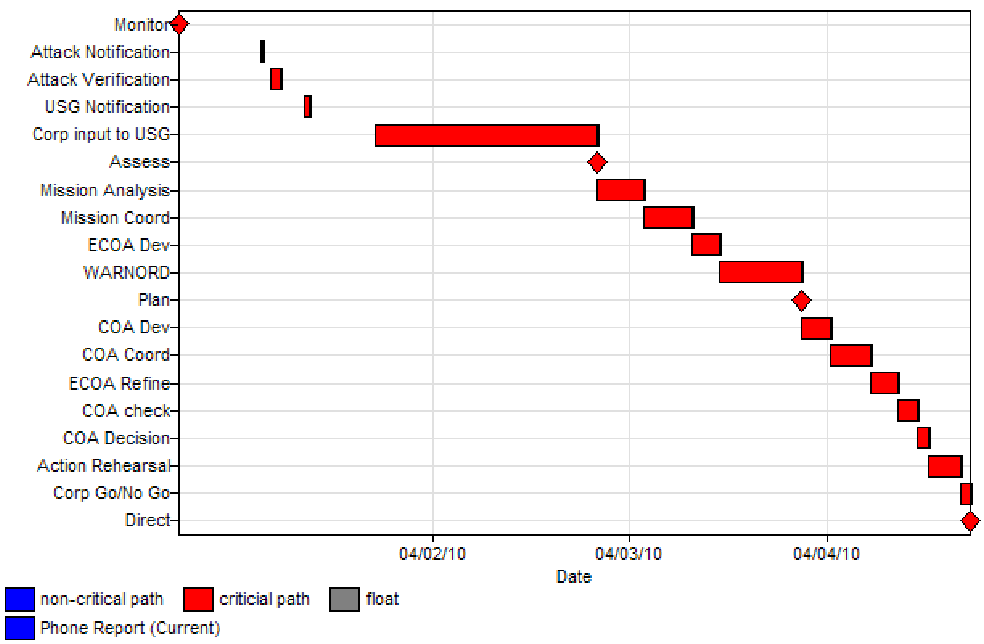

Figure 17. Gantt Chart for the current reporting configuration

The "As Is" configuration provides several insights into decision making processes when current technologies and architectures are used. Perhaps the most

important piece of information resulting from this experiment is the Simulation Duration. This is represented as the horizontal axis of the chart in Figure 17 which is contrasted against the individual tasks that make up the vertical axis of Figure 17. The Simulation Duration for this experiment was 96 hours and 28 minutes. This is the mean of 10,000 runs and there is a standard deviation of 3 hours and 53 minutes. The default repetition setting in the POW-ER model is 100, this was increased to 10,000 in order to ensure proper inferences could be made about the population (all MOC users) from this sample (actors in the model). The notional start date for this experiment was April 1, 2010. The simulated end date occurred on April 4, 2010.

Another statistic important in interpreting Figure 17 is Direct Work. Direct Work represents the "critical path" and which is depicted in red. The critical path denotes the logical flow of work from start to finish with no re-work. The Direct Work for this experiment is 36 hours and 40 minutes. There is no deviation for Direct Work due to the design of the tasks in the model. Should the task not be completed in its allotted amount of time it is then considered Re-Work. Direct Work within the model occurs in a linear fashion, meaning all Direct Work (work in the critical path) stops until the Re-Work is completed. The mean Re-Work for this experiment is 19 minutes with a deviation of one hour 52 minutes. The mean deviation is so low due to the infrequency of its occurrence (0.01 of 10,000 runs). The Re-Work is represented as "float" in Figure 17.

When considering factors that either contribute to or detract from the timeliness of reporting incidents of piracy within a command and control system the amount of time required to complete specific tasks must be taken into account. In the experiment using the "As Is" configuration the task identified as "Corp Input to the USG" is the most time intensive. The mean duration for this task in this experiment is 27 hours. The deviation of the duration for this task is three hours and 32 minutes. The Direct Work required to complete this task is 24 hours with a deviation of nine minutes.

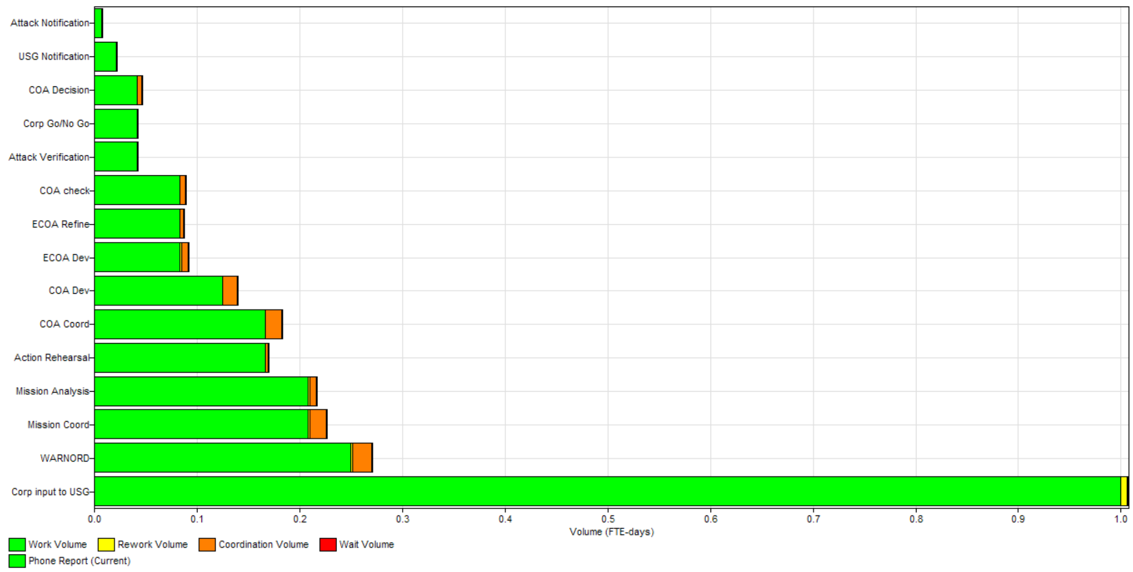

Figure 18. Task Duration in Days

The duration of other tasks specific to this experiment and the work required to complete these tasks must be taken into account. The duration of these tasks is broken down in Figure 18. The vertical axis of Figure 18 is labeled by the name of the individual task. The horizontal axis is labeled as Volume in terms of FTE-days (as defined in Chapter III). This translates to time as fractions of a 24 hour day. The duration of tasks unique to each model will yield the most information. The duration of tasks shared between both experiments are less valuable since their variance lies at the fourth significant digit. This translates to a difference of mere seconds.

The task representing the notification of the ship-owner for this configuration is labeled "Attack Notification" in Figure 18. The mean duration of this task is 12 minutes with no deviation over the 10,000 runs. The duration of the Direct Work required to complete is ten minutes with a deviation of three seconds. The task labeled "Attack Verification" accounts for the company's attempt to identify false alarms; this task has a mean duration of one hour and seven minutes. There was no deviation of the duration of this task in this experiment. The Direct Work required to complete this task is one hour. During the experiment there was a deviation of the Direct Work equaling 25 minutes. The last task specific to the "As Is" configuration of this model is the "USG Notification" task. This task represents the initial contact made between the shipping company and the

U.S. government. The mean duration of this task is 34 minutes with zero deviation. The duration of the Direct Work for this task is 30 minutes, with a deviation of only ten seconds. The combined duration of the tasks unique to this experiment is one day four hours and 53 minutes.

2. "To Be"

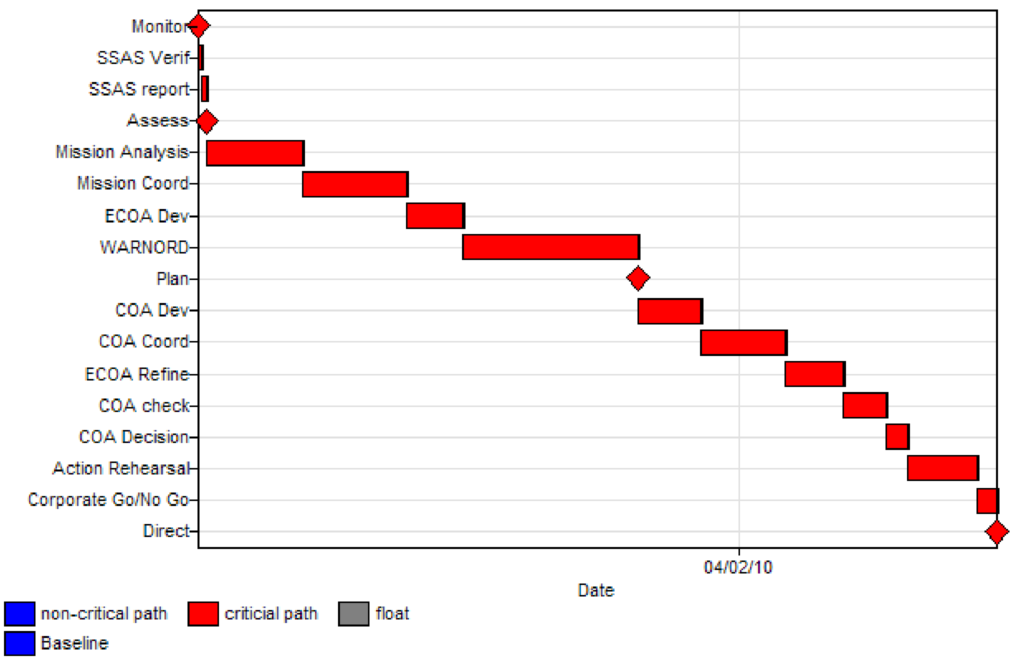

Figure 19. Gantt chart for the desired reporting configuration

The "To Be" configuration of the POW-ER model provided data points that, when properly examined, can offer means to improve the U.S. Navy's methods for receiving notification of pirate attacks. Much can be revealed from the statistic Simulation Duration in this model. The Simulation Duration for this experiment has a mean of one day, 21 hours and 50 minutes. This experiment consisted of 10,000 runs using this configuration and had a standard deviation of one hour and nine minutes. The Direct Work for this experiment had a mean duration of one day, 11 hours and 20 minutes. The Simulation Duration is represented as the horizontal axis of Figure 19. The Direct Work is shown in red and is labeled as "critical path" in Figure 19. The deviation for Direct Work was zero. The Re Work for this experiment accounts for any task not

completed upon its first attempt and is represented in Figure 19 as “float.” The Re Work for this experiment had a mean of nine minutes with a standard deviation of 52 minutes.

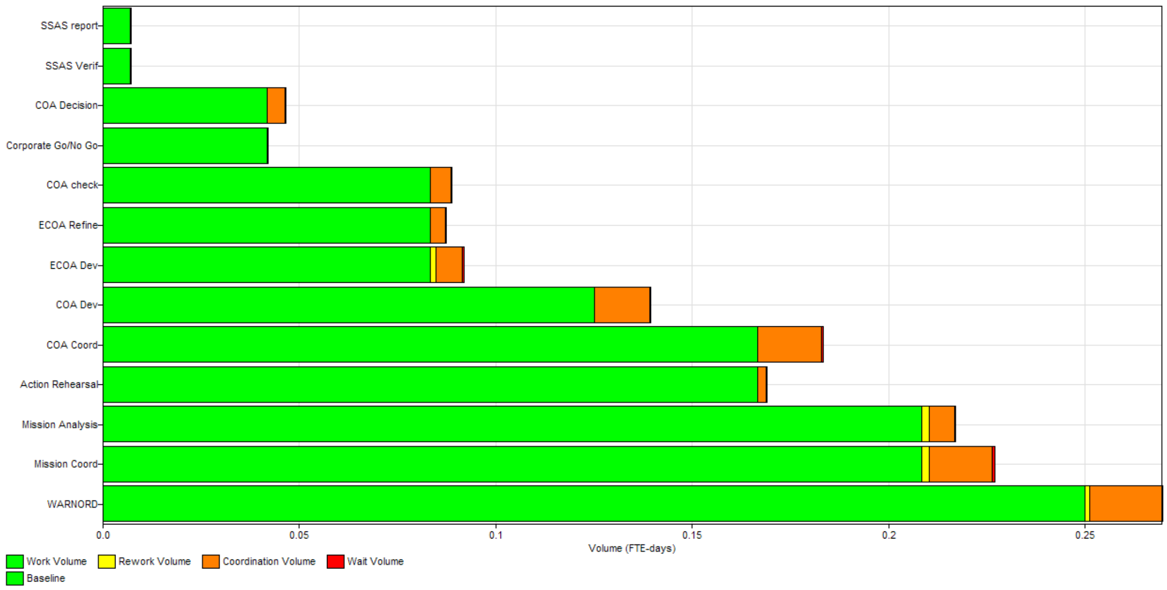

Figure 20. Task Duration in Days

Figure 20 displays the work volume in terms of FTE days for each specific task in the “To Be” Experiment. The most time intensive task for this experiment is the generation and issuance of the Warning Order (WARNORD). The mean duration of this task was ten hours and two minutes. The standard deviation for this task was ten minutes. Unique to this experiment were the tasks “SSAS report” and “SSAS Verif.” Both the tasks “SSAS report” and “SSAS Verif” had a mean duration of 12 minutes and a standard deviation of 11 seconds. The Direct Work associated with each of these tasks had an equal mean duration of ten minutes and a standard deviation of three seconds. The combined duration of all the tasks specific to this experiment is ten hours and 26 minutes.

B. DATA ANALYSIS/KEY FINDINGS

1. Scenario Tasking and Its Impact on Results

Tasks specific to the "As Is" and those specific to the "To Be" experiment offer the clearest insight into the overall time required to respond to incidents of piracy. These tasks highlight the differences in the reporting processes between ships and the U.S. government. The tasks shared by both configurations are the same as they are tasks carried out as the assessment and planning phases of the response. Keeping these tasks the same offers added control in the experiment. The sum of the tasks unique to the "As Is" experiment is 28 hours and 53 minutes. This is 18 hours and 27 minutes longer than the time required to complete the tasks unique to the "To Be" experiment. The "To Be" experiment had a mean duration of ten hours and 26 minutes for tasks unique to its configuration.

In the case of the "As Is" configuration, the most time intensive task is the corporation's input to the U.S. government, which has a mean duration of 27 hours. This is 16 hours and 58 minutes longer than the most time intensive task for the "To Be" configuration. The generation of the Warning Order has a mean duration ten hours and two minutes and is the most time intensive task of the "To Be" configuration. The Warning Order having the longest duration is significant due to the fact it is a task in both configurations, thus it cannot be avoided.

2. Backlog

The backlog within an experiment shows where the sequence of tasks slows or stops due to the action/inaction of a specific position. It is measured in terms of percent vs. time. This is useful when contrasting operational changes within a C2 structure. In the experiment modeling the current reporting system (As Is), the greatest backlog occurs when the shipping company via the Company Security Officer must provide initial notification and input to the U.S. government. This backlog reaches 100% in the first simulated day. In the experiment modeling the "To Be" reporting system, the greatest backlog achieved was measured at 42.66%, this was caused by the U.S. government position while completing the task "Mission Coordination."

The reduction in the highest backlog is significant because the Mission Coordination task is in both experiments. Logically the U.S. government backlog in the "As Is" experiment was measured at 42.64%, resulting in a mean difference of 0.02% between experiment configurations. It can then be stated that the impact of removing the Company Security Officer's backlog directly results in a time savings of 27 hours with a deviation of nine minutes.

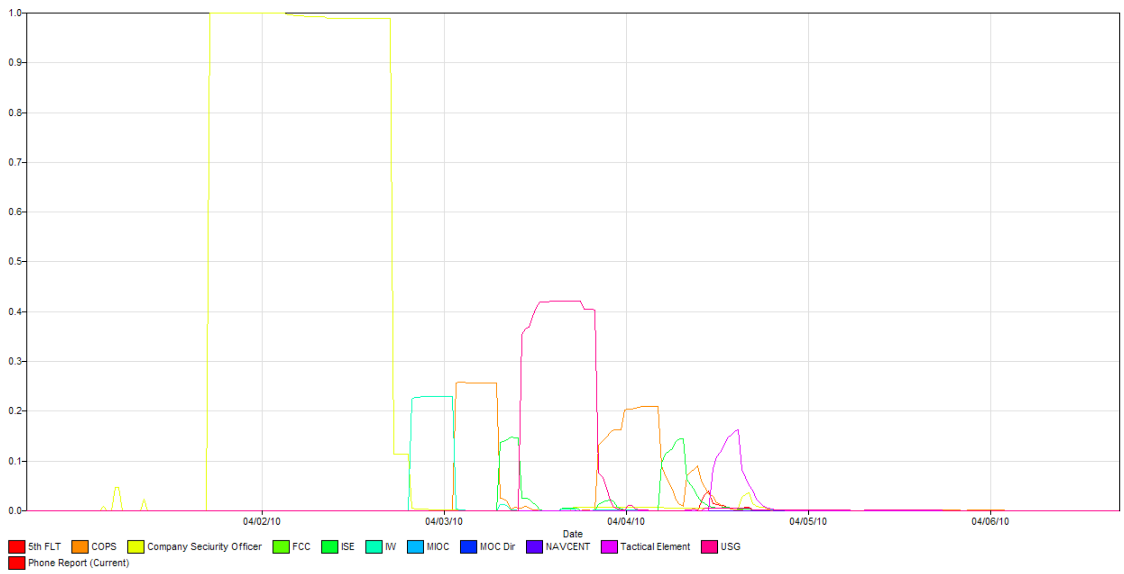

Figure 21. Position Backlog for "As Is" configuration

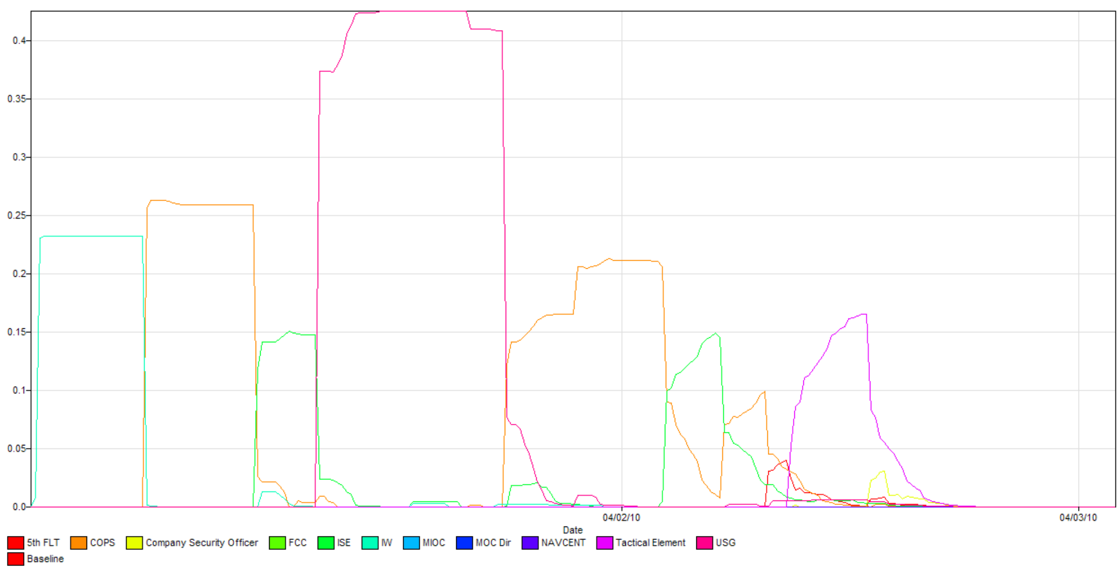

Figure 22. Position Backlog for "To Be" configuration

C. IMPLICATIONS

The small changes to the C2 structure for reporting incidents of piracy led to the decrease in the time the USN can dispatch ships to intercept the pirated vessel and decreased the time it takes for the MOC to plan an operation to retake the pirated vessel. The technologies inject with SSAS and a change in notification from the shipping company's Security Officer to the I&W watch floor team at the MOC has impact on two different timelines. The first timeline is the time it takes to notify USN ships in order to intercept the pirated vessel and the second timeline is the time it takes the USN to develop a plan to present to the shipping company to retake the ship.

The "To Be" scenario is an accurate and consistent command structure for the operational level of war. The proposed MOC construct offers the benefits of timely data and accurate information on a consistent basis. Reassurance of a consistent response could allow the MOC to replace presidential involvement further decreasing the time to response. Presidential involvement was prevalent in previous instances of piracy against U.S. shipping such as with the *Alabama* and in the 1800s against the Barbary Pirates, however, it was the on-scene-commanders' assessment of the situation that decided the action. The "To Be" model with a faster time to plan and earlier intercept allows greater opportunity to carry out commander's intent by the on-scene-commander.

The decrease in time with the "To Be" scenario enables an optimization of force placement to counter individual acts of piracy vice happening to be in close proximity as an attack happens. Over time trends in pirate attacks can be analyzed to preposition USN ships. Positioning of these ships can now be based upon the "To Be" model which reduces the time to plan and respond. Given a reduction in time required to respond, fewer numbers of U.S. ships are required to cover the ever increasing area of pirate operations. Optimized force placement can extend protected shipping lanes which can challenge the pirates' ability to conduct long range operations. A condensed response time could have prevented the botched hostage exchange of Captain Phillips of the *Alabama* incident.

In the "To Be" model, the inject, of SSAS provides geographic location of the pirated ship as well as more timely reporting directly to the MOC. The known location and other near real time information such as ships course and speed could have benefitted the recovery of the *Achille Lauro*. The inability to track and report the ships position hindered U.S. planners to dispatch forces. This inability prevented an early and visible U.S. presence that might have saved the life of Leon Klinghofer.

Further implication of the "To Be" model is that it can stand as the C2 structure for response to a U.S. merchant ship involved in an incident of piracy in any AOR. As USN numbered fleets implement their MOCs, global U.S. shipping deserves a consistent response from fleet to fleet. Implementation of the "To Be" model in all USN numbered fleets would guarantee this consistent response. A reliable and consistent response yields greater cooperation with shipping companies notably foreign owned companies with U.S. flagged shipping. Success of these responses would urge foreign navies to standardize their responses allowing for greater cooperation in coalition efforts to respond to piracy.

1. Factors Affecting Timing

There are several critical events associated with a successful pirate attack on a merchant ship. There is the time the attack begins, the time the ship is taken, the time the USN is notified (in order to vector USN ships to the merchant ship), and the time the merchant ship, under the control of pirates, begins its return to one of the Somali ports. The below figure is a timeline representing critical times in order of occurrence and a legend of the variables that represent each critical time.

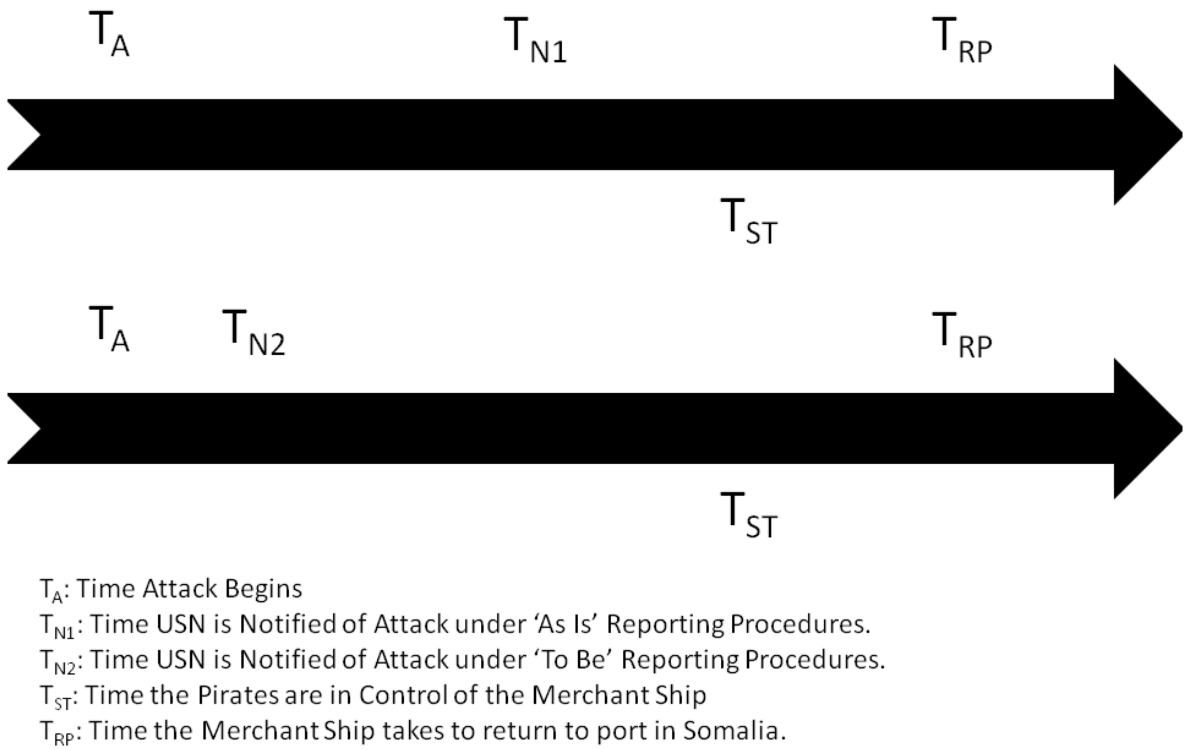

Figure 23. Timeline of Critical Times associated with a successful pirate attack.

The time of notification in this instance is assumed to be the time the USN is notified of the incident and can dispatch surface ships to intercept the pirated vessel but cannot retake the ship. This first timeline shows that $T_{N1} > T_{N2}$. T_{N1} = Attack Notification + Attack Verification + USG Notification. T_{N2} = SSAS Notification + SSAS Verification. These establish the variable T in a classic time/distance problem where:

$$D = R * T$$

Where D = distance in nautical miles, R = Rate in knots and T = time measured in hours and minutes. The rates involved are those of the pirated vessel and those of USN ships dispatched to interdict the pirated vessel. In nearly all instances the Rate of the USN ship is greater than that of the pirated vessel such that $R_{USN\ Ship} > R_{Pirated\ Vessel}$. Classically the pirates have relied on a large T_{N1} (time to notification), while the USN has

relied on heavy concentration of forces and small variation in $R_{Pirated\ Vessel}$. This model highlights the reduction in time to T_{N2} to decrease the distance to intercept pirated vessels.

According to results from the simulation T_{N1} = 12 minutes + 1 hour and 7 minutes + 34 minutes = 1 hour and 53 minutes. T_{N2} = 12 minutes + 12 minutes = 24 minutes. The implications of this are illustrated in the following scenario of a pirated vessel steaming back to port at 15 knots. Fifteen knots was chosen to reflect the top speed at which a U.S. flagged motor vessel could steam with engineers under duress. Looking at this from a classic time/distance problem we have the following distances the pirated vessel could cover with the two different notification times:

$$D = R * T$$

Where D = distance in nautical miles, R = Rate assumed to be 15 knots and T = time measured in hours and minutes.

$$D = R * T_{N1} = 15 \text{ knots} * 1 \text{ hour } 53 \text{ minutes} = 28.25 \text{ nm}$$

$$D = R * T_{N2} = 15 \text{ knots} * 24 \text{ minutes} = 6 \text{ nm}$$

"As Is" reporting procedures utilizing T_{N1} have the pirated vessel traveling approximately 28 nm whereas "To Be" reporting procedures utilizing T_{N2} have the pirated vessel traveling approximately 6 nm. These relatively small distances would have a large impact in the crowded waters of the GOA. In the vast expanse of the Indian Ocean these small distance gains can be exploited by optimally positioned surface forces.

The second timeline involving the Navy's ability to run through the planning process to develop a course of action in approximately half the time from the "As Is" case to the "To Be" case. The ability to be notified of an incident of piracy, develop a plan and brief that plan to the civilian shipping corporation is approximately 96 hours under the "As Is" architecture. That time is approximately 48 hours under the "To Be" Architecture. Using the previous time/distance problem with the same rate of 15 knots

but using 96 hours for the time in the "As Is" problem and 48 hours in the "To Be" problem the following distances were calculated:

$$D = R * T$$

Where D = distance in nautical miles, R = Rate assumed to be 15 knots and T = time measured in hours and minutes.

$$D = R * \mathrm{T} \quad = 15 \text{ knots} * 96 \text{ hours} = 1{,}440 \text{ nm}$$

$$D = R * \mathrm{T} \quad = 15 \text{ knots} * 48 \text{ hours} = 720 \text{ nm}$$

Interdiction of a pirated vessel is feasible in terms of having an asset on scene to provide situation reports as events unfold or serve as a platform to launch operations from against the pirated vessel. The USN has proven capable of dispatching forces upon receiving word of a pirate attack all too often arriving on scene awaiting further orders to resolve the situation. The real time savings of the "To Be" model provide the ship and the on-scene commander guidance that previously suffered significant time delays. The above numbers involving the ability of the USN to run through the planning process provide a staggering decrease in the amount of time the USN can develop a plan and have designated forces ready to carry out that plan. The "As Is" C2 structure has a plan being delivered approximately 96 hours after the notification of a successful pirate attack, giving the pirates a range of about 1,440 nm at 15 knots to return to port.

The "To Be" timeline has significant time savings from notification of the pirate attack until a plan is prepared and units are identified and designated. The time duration for the "To Be" C2 architecture is approximately 48 hours, which for the pirates steaming at 15 knots is a range of 720 nm. The changes to the C2 structure from the "As Is" to the "To Be" can seriously impact long range pirate activities. An unintended consequence of current anti-piracy operations was driving pirate activities further from the coast of Somalia with documented attacks occurring 1350 nm east of Mogadishu. Under the "As Is" C2 structure the pirated vessel could return to port before the planning process could be finalized. Under

the “To Be” C2 structure a plan to retake this vessel could developed and ready to execute while the pirated vessel is still approximately 700 nm off the coast of Somalia.

The direct notification of a pirate attack to the MOC I&W cell means that long-range pirate activities greater than 800 nm off the coast of Somalia can have Navy assets ready to execute the direction given by the MOC planners while the vessel is still approximately 100 nm off the coast and 88 nm outside of territorial waters. According to results from the International Maritime Bureau (IMB), there were approximately 65 successful or attempted attacks in 2010, IVO Gulf of Aden and the Indian Ocean, current as of 12 May 2010. Forty-eight of those attacks occurred in the Indian Ocean and of those 48 approximately 34 attacks occurred (12 of which were successful) at a distance near 800 nm from Mogadishu. This thesis recognizes that pirated vessels return to several port towns in Somalia, to include Mogadishu, but for the purposes of statistical analysis Mogadishu serves as a central geographic location with pirate towns to the north and south of Mogadishu. The below graphic shows a range ring of approximately 800 nm from Mogadishu showing which pirate attacks fall within that ring and which fall outside of it.

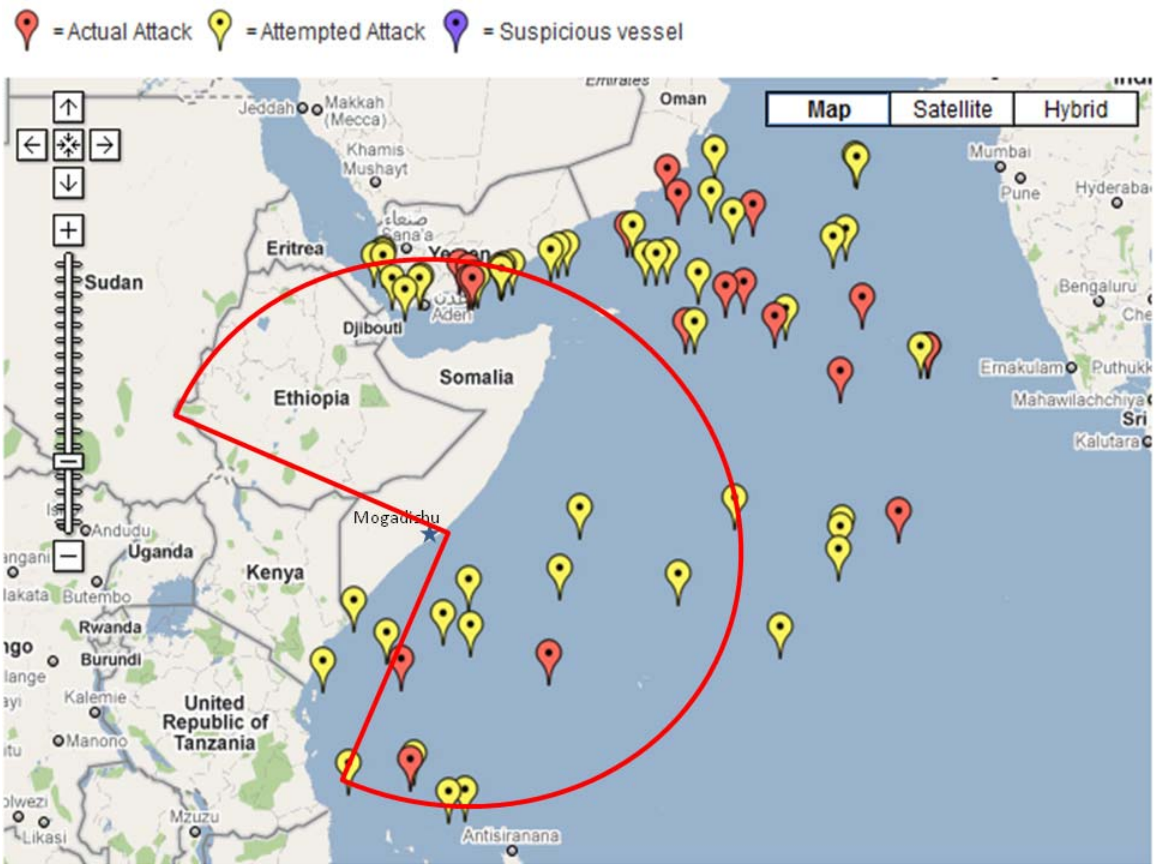

Figure 24. Pirate Attack Reporting Map (From International Maritime Bureau, 2010)

Thirty-four out of 48 attacks fell outside of 800 nm from Mogadishu or 71% of attacks in the Indian Ocean occurred outside of 800 nm. According to the simulation run the USN could have gone through the planning process and have forces ready to execute a plan for 71% of all pirate attacks in the Indian Ocean before they were able to return to port. Twelve out of 34 of those attacks were successful and occurred outside of 800 nm from Mogadishu or 35%. If these successful attacks were reported through the "To Be" C2 structure the USN could develop courses of action to present to the shipping company and be ready to execute those orders before the pirated vessel returned to port.

2. Hypothetical Application

It is important to put the results of these experiments in the context of possible future attacks on merchant shipping by pirates. A notional scenario involves a U.S. flagged container ship steaming off the coast of Somalia. This ship is attacked and driven

toward the pirate town of Harardhere 863 nm from the attack. The ship is moving at a speed of 15 knots. There are two U.S. Navy surface ships in the area, USN Ship 1 is 361 nm from the attack. USN Ship 2 is 544 nm from the attack. It is assumed the U.S. Navy ships are capable of making 30 knots to intercept the pirate ship.

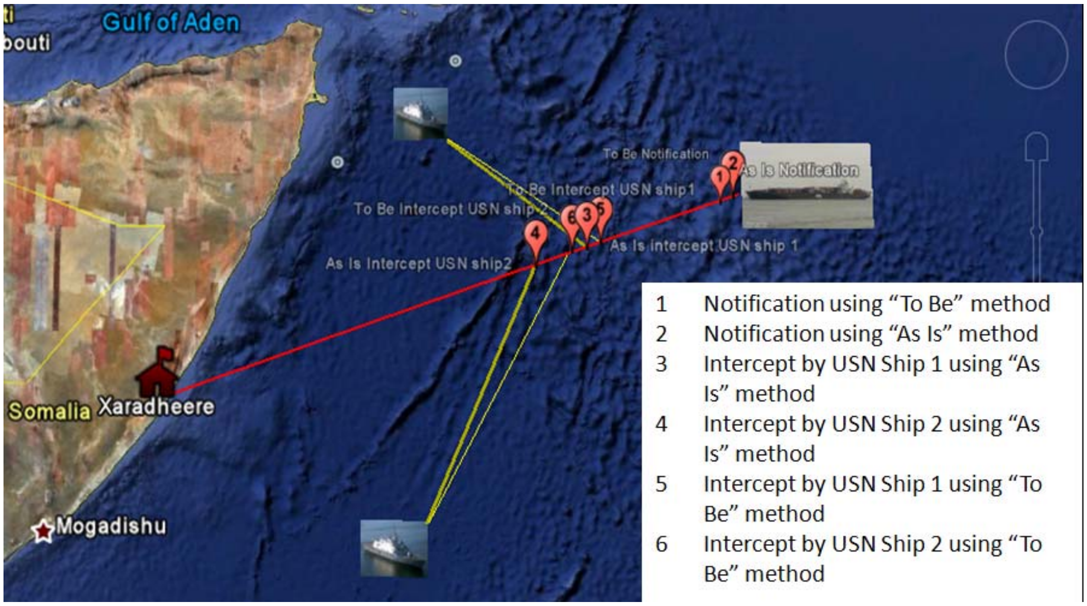

Figure 25. Hypothetical scenario (Google Earth, 2010)

In this scenario using the "As Is" reporting architecture, the time between the attack and notification of the U.S. government is one hour and 53 minutes. Given an estimated speed of 15 knots, the pirate ship will have traveled 28.25 nm down its track to Harardhere during this time period. Using the "To Be" method of notification 24 minutes elapse between the attack and U.S. government notification. At a speed of 15 knots, this means the victim ship would only travel six nautical miles towards Harardhere.

Assuming U.S. Navy ships are dispatched instantly upon notification and steaming at a speed of 30 knots U.S.N., ship 1 must travel 238 nm to intercept the victim ship using the "As Is" reporting architecture. This will intercept the victim ship 246 nm from the site of the attack. Under the proposed "To Be" reporting architecture, the U.S.N. ship 1 would travel 267 nm at a speed of 30 knots to intercept the vessel 211 nautical miles from the site of the attack.

	As Is	To Be
Time to Notification	1 hour 53 minutes	24 minutes
Time to Intercept	7 hours 56 minutes	8 hours 54 minutes
Dist to Intercept	238 nm	267 nm
Intercept distance from Attack site	246 nm	211 nm
Time to Direction from U.S. N.	4 days 28 minutes	1 day 21 hours 32 minutes

Table 1. U.S.N. ship response and interception

The direct benefits of the proposed "To Be" configuration are not immediately apparent. The time to intercept and the distance required to travel to intercept are longer under the "To Be" architecture, however the time of notification, and the distance from the attack site is shorter. Therefore there are modest gains to be made in this earlier notification and dispatch of vessels in the area. The most significant gains are realized when the theater-wide response is taken into account.

The time required to enact a plan developed is represented when the "Direct" milestone is met. The time to "Direct" is equal to the Simulation Duration. The time to Direct under the "As Is" configuration is 96 hours and 28 minutes. The time required for the victim ship to be successfully maneuvered back to Harardhere is 57 hours and 32 minutes. Therefore the victim ship will have been in the pirate's port for one day 14 hours and 28 minutes. The time to Direct in the "To Be" configuration is one day four hours and 53 minutes. This direction comes with 152 nm remaining before the pirates reach Somali territorial waters.

Figure 26. Scenario times of notification and direction (Google Earth, 2010)

The advantage of intervention so far out to sea is the extension of lines of communication and supply on the part of the pirates. Any attempts to resupply the pirates or get them off the ship will be apparent to U.S. Forces. This further aides the United States in controlling either the terms of surrender or the negotiations of moneys to be paid. The other advantage of countering acts of piracy in international waters is the ability to act unilaterally with only the permission of the shipping company required. The issue of military action by the United States on a commercial vessel in a sovereign country's territorial waters is avoided altogether. Given the safe transit routes through waters near Somalia and the tightening grip of EU and U.S. Navy forces in those waters attacks with an ever increasing range from Somalia is highly likely. As of March 12, 12 of 48 attacks in 2010 have occurred at a distance of 800 nm or more from Somalia.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. SUMMARY

Spikes in events of piracy have been increasing since 2006, and the international community can no longer ignore this problem. Legal, socio-economic, and technological issues hinder multi-national efforts to combat piracy effectively. Response to events of piracy are oftentimes late, as reporting of incidents is also mired in legal issues; however, technology does exist that can notify companies that a ship is being attacked by pirates as the attack occurs.

Though communications technology evolved greatly between the times of Decatur's Mediterranean Squadron and the *Mayaguez*, the response by the Ford Administration was mired by unnecessary complexities in the reporting structure. This became evident at the initial notification of the attack on the *Mayaguez*. Initial notification had to be relayed three times, resulting in a six-hour delay between initial notification of the attack and notification of President Ford. The complex web of communication required to direct tactical forces must be streamlined to provide an agile response.

Small changes to the processes within the C2 structure can transform piracy reporting from the "As Is" piracy reporting process to the "To Be" reporting process, effectively halving the time required to give tactical direction. These changes to processes are made possible in this case by both technologies currently used and commercially available technology not currently used by the DoD. The enabling technology in this case, is the Ship Security Alert System (SSAS) and The International Maritime Organization (IMO) has mandated that all ships greater than 500 gross tons (United States Coast Guard, 2004) shall be equipped with an SSAS. The problem lies in who should receive the SSAS attack alert notification. Currently, these distress signals only go to the company that owns the ship. With the increase in frequency and range of these attacks, the Operational-level commander must have as much pertinent information

as soon as possible. A direct inject of SSAS information into a Navy Maritime Operations Center will enable a faster response time to piracy events and allow for trend analysis of where pirate attacks are occurring.

This thesis was able to show the benefits of streamlining reports to the U.S. Navy's 5th Fleet MOC. These benefits were shown using the POW-ER modeling software. POW-ER is an inexpensive method to model organizational structures yielding quantitative data. Given the demands on personnel actively responding to ongoing acts of piracy, it was not feasible to physically demonstrate the hypothesis of the thesis in the real-world. POW-ER stands as an efficient way to expand the scope of this research by looking at other areas the C2 structure can be streamlined in reporting and responding to incidents of piracy.

The direct notification of a pirate attack to a Maritime Operations Center means pirate activities greater than 800 nm off the coast of Somalia will face Navy assets ready to execute the direction given by MOC planners while the vessel is still approximately 100 nm off the coast and 88 nm outside of territorial waters. According to results from the International Maritime Bureau (IMB), there were approximately 65 successful or attempted attacks in 2010, in the vicinity Gulf of Aden and the Indian Ocean, current as of 12 May 2010. Forty-eight of those attacks occurred in the Indian Ocean, of which 34 occurred at a distance near 800 nm from Mogadishu, and of these, 12 were successful. This thesis recognizes that pirated vessels return to several port towns in Somalia, to include Mogadishu, but for the purposes of our statistical analysis, Mogadishu serves as a central geographic location with pirate towns to the north and south of Mogadishu.

B. AREAS FOR FUTURE RESEARCH

The United States stands ready to repel these pirates and but needs the capable and available tools to execute the mission. Although this thesis outlines the advantages of a Command and Control system using SSAS, there are many aspects of implementation that remain to be studied. Some of these aspects include:

1. Interface requirements between existing DoD/DON networks and commercially available SSAS systems.

2. Legal ramifications of compliance to reporting regulation by U.S. flagged merchant shipping.

3. Role of the U.S. Coast Guard in enforcing standards for maintenance and operability of SSAS systems aboard U.S. flagged merchant ships.

4. Model existing Somali pirate C2 structures in POW-ER to identify critical areas of weakness for exploit by U.S. forces.

5. Benefit analysis of lower echelon commanders being given operational tasking authority; previous singular incidents of piracy involving U.S. shipping has required tasking from the President of the United States.

6. Cost benefit analysis of re-flagging foreign flagged ships (e.g. insurance savings).

7. Means of force optimization within the HOA AOR given the time savings discovered through C2 changes in this thesis.

For all the variability in the battle against maritime piracy, the constant that stands head and shoulders above the rest is the need for quick and effective command and control processes. These processes must come from streamlined hierarchical organization. With advances in both ship monitoring and communication, commercial shipping companies and the U.S. Navy must forge a strong partnership to share information to prevent and react to pirate attacks. Using the ideas posited in this thesis to streamline reporting and optimize U.S. Navy asset placement will help tip the balance of this fight back in favor of those seeking to use the sea for legitimate commerce.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Ahmed, M. (2009, December 01). *Reuters*. Retrieved December 10, 2009, from http://www.reuters.com/article/africaCrisis/idUSGEE5AS0EV

American merchant marine at war. (2000). *Capture and Release of SS Mayaguez by Khmer Rouge forces in May 1975.* Retrieved February 17, 2010, from The American Merchant Marine at War: http://www.usmm.org/mayaguez.html

Bahadur, J. (2009, April 16). *East Africa forum*. Retrieved October 13, 2009, from http://www.eastafricaforum.net/2009/04/23/im-not-a-pirate-im-the-saviour-of-the-sea/

Barrett, F., & Nissen, M. (2008). Self organization and synchronization at the edge: Situated action, identity and improvisation. *International Command and Control Research and Technology Symposium* (pp. 1–18). Monterey, CA: Naval Postgraduate School.

BBC. (2002, May 7). *H2G2*. Retrieved February 15, 2010, from BBC: http://www.bbc.co.uk/dna/h2g2/A730900

Chairman of the Joint Chiefs of Staff. (1975). *After action report: U.S. military operations S.S. Mayaguez/Kaoh Tang 12–15 May 1975.* Washington, D.C.: Joint Chiefs of Staff.

CJCS. (1995). *Joint publication 6.0.* Washington, D.C.: JCS.

Commons, H. (2010, January 17). *Military affairs>> personell*. Retrieved February 1, 2010, from History Commons: http://www.historycommons.org/topic.jsp?topic=topic_personnel

Creveld, M. V. (1985). *Command in war.*Cambridge: President and Fellows of Harvard College.

DeKay, J. T. (2004). *A rage for glory: The life of commodore Stephen Deatur USN.* New York: Free Press.

Department of the Navy. (2000). *The U.S. Navy in the Cold War Era, 1945–1991*. Retrieved February 15, 2010, from U.S. Navy Heritage and History Command: http://www.history.navy.mil/wars/coldwar-1.htm

Department of the Navy. (2008). *Maritime Operations Center NTTP 3-32.1.* Newport, RI: Department of the Navy.

Dillon, D.R. (2005) SAIS Review. Retrieved January 5, 2010, from: http://muse.jhu.edu/journals/sais_review/v025/25.1dillon.html

Elliott, B. J. (2009, April 30). *Klein: "Peace partner" helped free terrorist who killed American. Leader of infamous Achille Lauro hijacking released yesterday from Italian prison.* Retrieved February 15, 2010, from RBO: therealbarackobama.files.wordpress.com/2009/0

Fraser, C. C. (1920). *Boys' book of sea fights.* New York: Thomas Y Crowell.

Google Earth. (2010, April 19). Google Earth. Retrieved April 10, 2010, from Google Earth: http//earth.google.co/gulfofaiden

Guilmartin, J. F. (1995). *A very short war: The Mayaguez and the battle of Koh Tang.* College Station : Texas A&M University Press.

Hunter, R. (2008, October 28). *Somali pirates living the highlife*. Retrieved January 12, 2010, from BBC News online: http://news.bbc.co.uk/2/hi/africa/7650415.stm

International Expert Group on Piracy off the Coast of Somalia. (2008). *Piracy off the Coast of Somalia.* Nairobi: United Nations.

International Maritime Bureau. (2010, April). *IMB piracy reporting center*. Retrieved April 19, 2010, from http://www.icc-ccs.org/index.php?option=com_content&view=article&id=30&Itemid=12

JMO Deparment, Naval War College. (2008). *Joint Operation Planning Process (JOPP) workbook.* Newport, RI: Naval War College.

Koburger, C. (2010). Selamat Datang, Kapitan: Post WWII piracy in the South China Sea. In F. R. Fellman, *Piracy and Maritime Crime: Historical and Modern Cases* (pp. 65-77). Newport, RI: Naval War College Press.

Leavitt, H. J. (1965). Applied organizational change in industry: Structural, technological and humanistic approaches. In H. J. Leavitt, *Handbook of organizations* (pp. 1144–1145). Chicago: Rand McNally.

Leiner, F. C. (2006). *End of Barbary terror: America's 1815 war against the pirates of north africa.* London: Oxford University Press, Inc.

Looney, J. P. (2006). Computational modeling and analysis of networked organizational planning in a coalition maritime strike environment. *2006 Command and Control Research and tech symposium: The state of the art and the state of the practice* (pp. 1–37). Monterey, CA: Naval Postgraduate School.

Malte-Brun, C. Barbary Coast. (1837). *Atlas Complet du Precis de la Geographie Universelle.* Paris: Aimé André, libraire-éditeur.

Marine Officer. (2009). Don't give up the ship! Quick thinking and a boatload of know-how saves the MAERSK ALABAMA. *Marine Officer*, *173*, 6–18.

Mojon, J.-M. (2009, October 29). *The Middle East online*. Retrieved December 01, 2009, from http://www.middle-east-online.com/English/?id=35360

Murphy, M. N. (2009). Chapter one: Contemporary piracy. *Adelphi Series 47:388* , 11–44.

Office of the Joint Seceratary. (1976). *CINCPAC Command History—Appendix VI—SS Mayaguez Incident.* San Francisco: Office of the Joint Seceratary Command History Branch .

Paust, J. J. (1976). The seizure and recovery of the Mayaguez. *Yale Law Journal, 84,* 774–806.

Ploch, B. O. (2008). *Piracy off the coast of Africa.* Washington, DC: Congressional Research Service.

Quérouil, M. (2008, October 27). *Saturnic's Journal*. Retrieved October 10, 2009, from http://saturnic.livejournal.com/346437.html

Rice, X. (2010, March 23). *The Guardian*. Retrieved April 19, 2010, from http://www.guardian.co.uk/world/2010/mar/23/somali-pirates-hijack-turkish-ship

Sundland, C. (2008). *Transforming data and metadata into actionable intelligence and information within the maritime domain.* Monterey, CA: Naval Postgraduate School.

United States Coast Guard. (2004). *Coast guard instruction 3120.3.* Washington, D.C.: United States Coast Guard.

Weaver, M. (2009, April 10). Somali pirates vow to take on U.S. military might if attacked. Retrieved February 5, 2010, from *The Guardian*: www.theguardian.co.uk/world/2009/apr/10/somali-pirates-hostage-us-military

Wireless, G. (2009). *Globe wireless, shipshape solutions*. Retrieved February 22, 2009, from http://www.seawave.com/solutions_list2_alert.php

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Secretary of the Navy
   Department of the United States Navy
   Washington, District of Columbia

4. OPNAV N3/N5
   Office of the Chief of Naval Operations
   Washington, District of Columbia

5. Naval Forces Central Command
   Manama, Bahrain

6. Joint and National Systems Division Surveillance Systems
   Space and Naval Warfare Systems Center
   San Diego, California

7. Program Executive Officer Command, Control, Communications, Computers, and
   Intelligence Space and Naval Warfare Systems Center
   Charleston, South Carolina

8. Dr. Dan C. Boger
   Naval Postgraduate School
   Monterey, California

9. Dr. Mark Nissen
   Naval Postgraduate School
   Monterey, California

10. Steven J. Iatrou
    Naval Postgraduate School
    Monterey, California

11. Jeffrey E. Kline
    Naval Postgraduate School
    Monterey, California

12. Daniel Warren
    Naval Postgraduate School
    Monterey, California